ISSACK WAITHAKA
cs-sa07-24085

Introduction

When analyzing malware we should note:

- - Point of entry
- - To check if malware has been executed on a machine
- - How does the malware perform
- - How to stop it

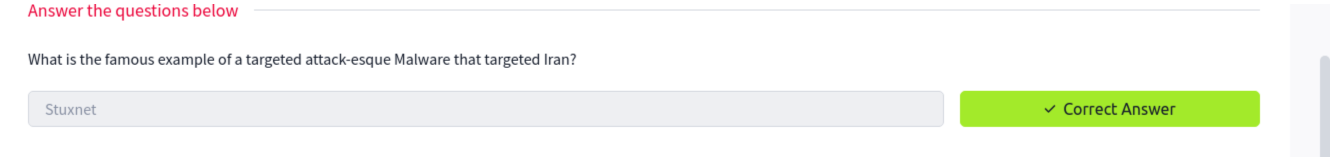
Understanding Malware Campaigns

- Targeted – this type of malware attacks are created for specific purpose against a specific target.

- Mass Campaign – its purpose is to infect as many devices as possible.

Questions

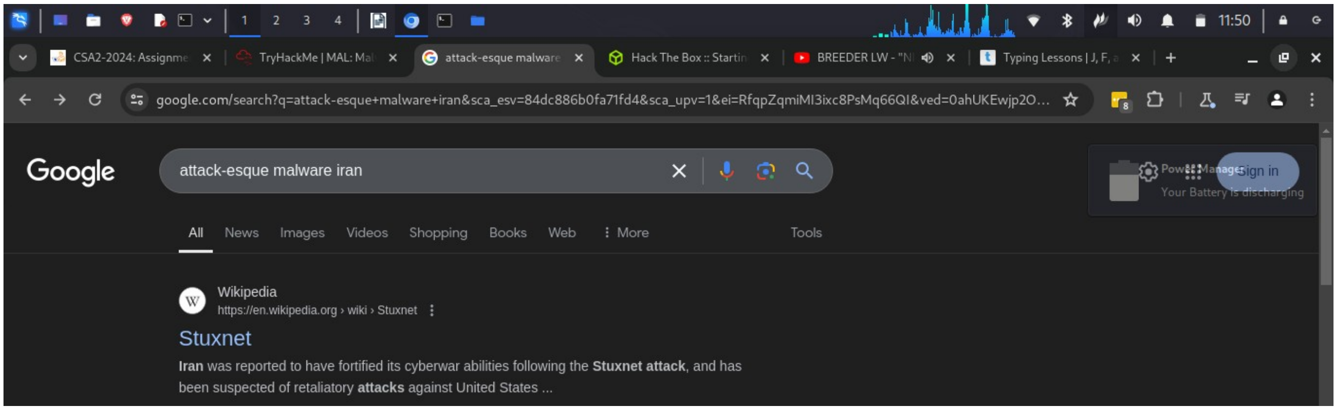
1.



Answer the questions below

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

Stuxnet



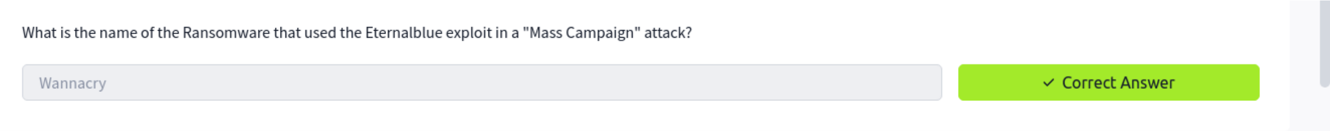
attack-esque malware iran

Wikipedia
https://en.wikipedia.org › wiki › Stuxnet

Stuxnet

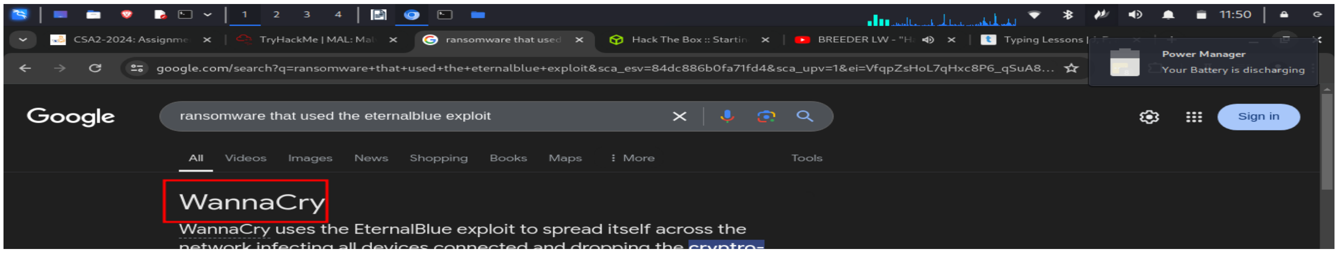
Iran was reported to have fortified its cyberwar abilities following the **Stuxnet attack**, and has been suspected of retaliatory **attacks** against United States ...

2.



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

Wannacry



ransomware that used the eternalblue exploit

WannaCry

WannaCry uses the EternalBlue exploit to spread itself across the network infecting all devices connected and dropping the cryptro-

Identifying if a malware attack has happened

- Malware attacks takes place in the following steps:

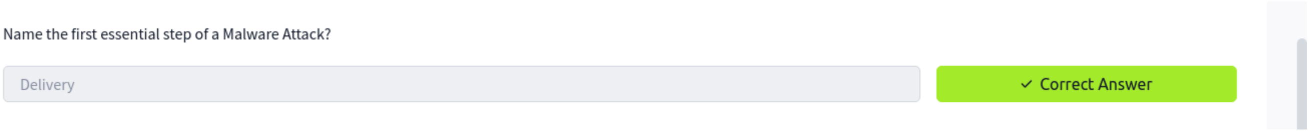
- - Delivery
- - Execution
- - Maintaining persistence
- - Propagation

Malware may leave behind two types of signatures which are:

1. Host-Base Signatures – These are the results of execution performed by the malware
2. Network-Based signatures – These are observations of any networking communication that took place

Questions

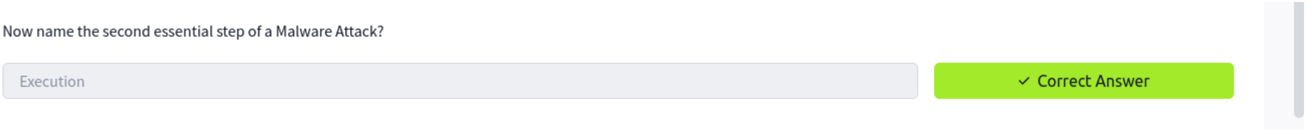
1.



Name the first essential step of a Malware Attack?

Delivery

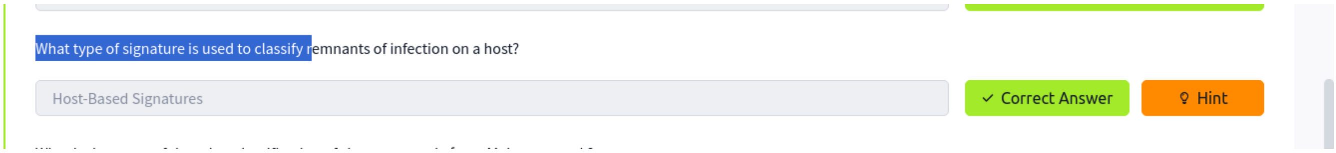
2.



Now name the second essential step of a Malware Attack?

Execution

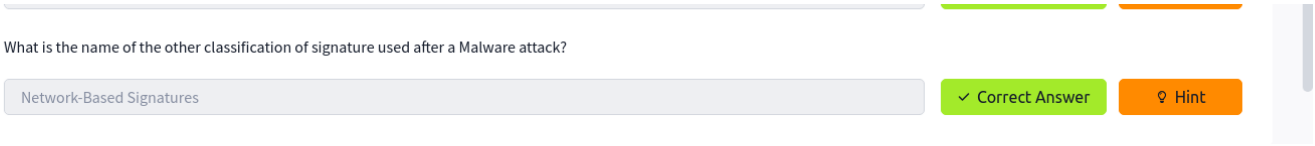
3.



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

Host-Based Signatures

4.



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

Network-Based Signatures

Static vs Dynamic Analysis

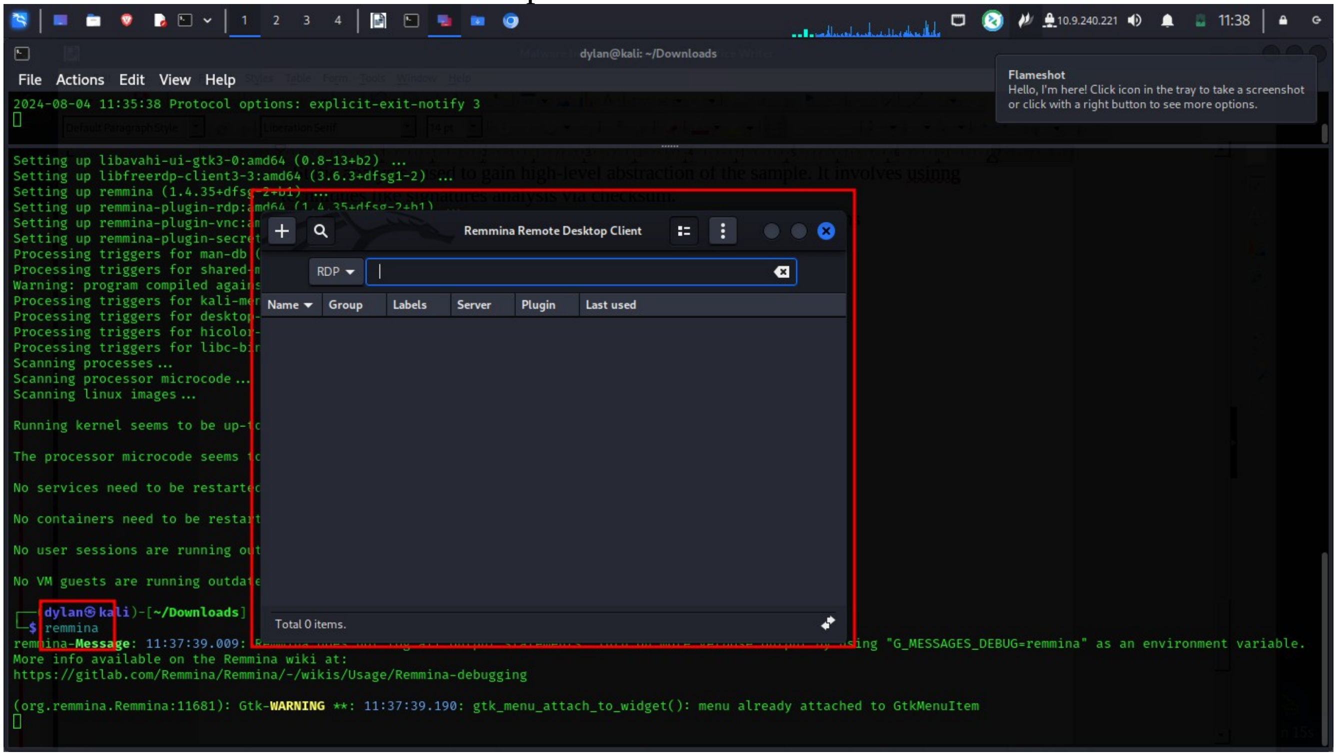
- Static analysis -used to gain high-level abstraction of the sample. It involves using techniques like signatures analysis via checksum.
- Dynamic Analysis – executing the sample and observing what happens

Discussion of provided Tools and their uses

- Here some tools we will use in the future were listed

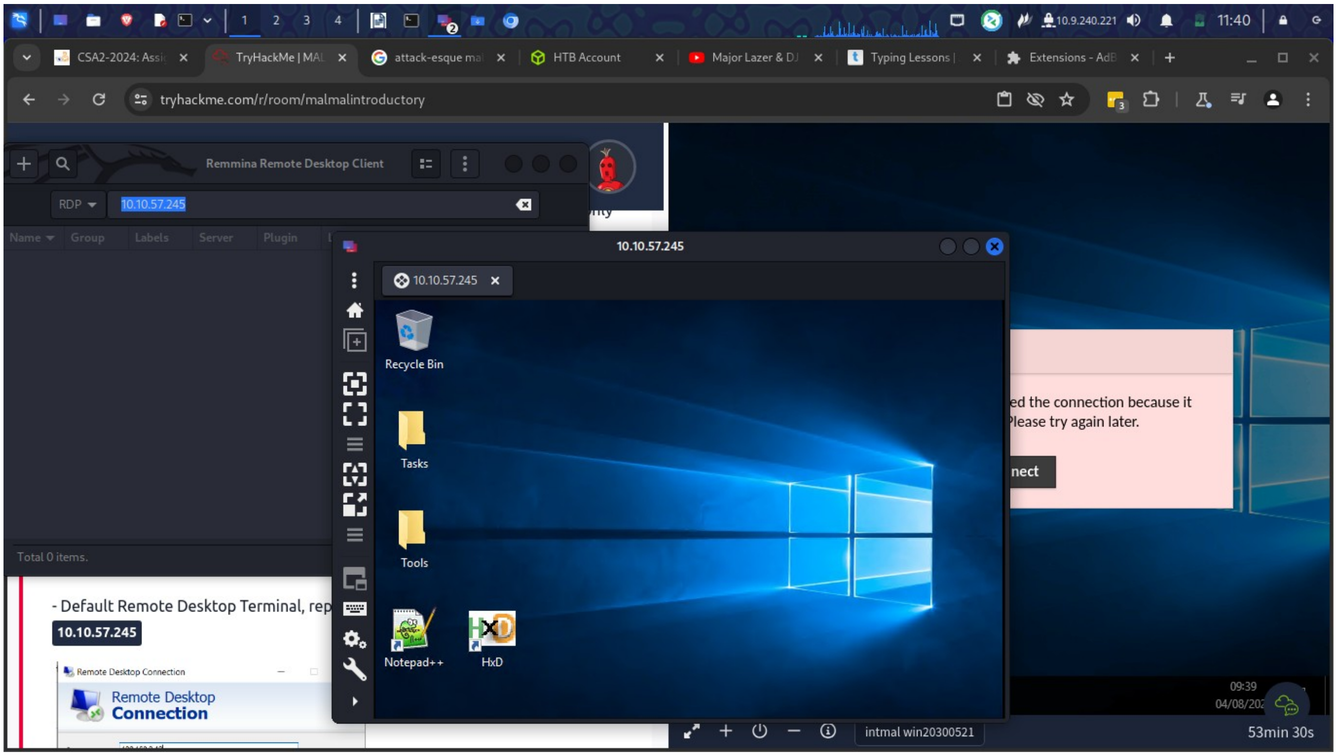
Connecting to the windows Analysis Environment (Deploy)

- I used remina to connect to the rdp



Flameshot
Hello, I'm here! Click icon in the tray to take a screenshot or click with a right button to see more options.

```
2024-08-04 11:35:38 Protocol options: explicit-exit-notify 3

Setting up libavahi-ui-gtk3-0:amd64 (0.8-13+b2) ...
Setting up libfreerdp-client3-3:amd64 (3.6.3+dfsg1-2) ...
Setting up remmina (1.4.35+dfsg-2+b1) ...
Setting up remmina-plugin-rdp:amd64 (1.4.35+dfsg-2+b1)
Setting up remmina-plugin-vnc:a
Setting up remmina-plugin-secre
Processing triggers for man-db
Processing triggers for shared-
Warning: program compiled agai
Processing triggers for kali-me
Processing triggers for desktop
Processing triggers for hicolo
Processing triggers for libc-b
Scanning processes...
Scanning processor microcode...
Scanning linux images...

Running kernel seems to be up-t

The processor microcode seems t

No services need to be restarte

No containers need to be resta

No user sessions are running ou

No VM guests are running outdat

┌──(dylan㉿kali)-[~/Downloads]
└─$ remmina
remmina-Message: 11:37:39.009: [illegible] using "G_MESSAGES_DEBUG=remmina" as an environment variable.
More info available on the Remmina wiki at:
https://gitlab.com/Remmina/Remmina/-/wikis/Usage/Remmina-debugging

(org.remmina.Remmina:11681): Gtk-WARNING **: 11:37:39.190: gtk_menu_attach_to_widget(): menu already attached to GtkMenuItem
```

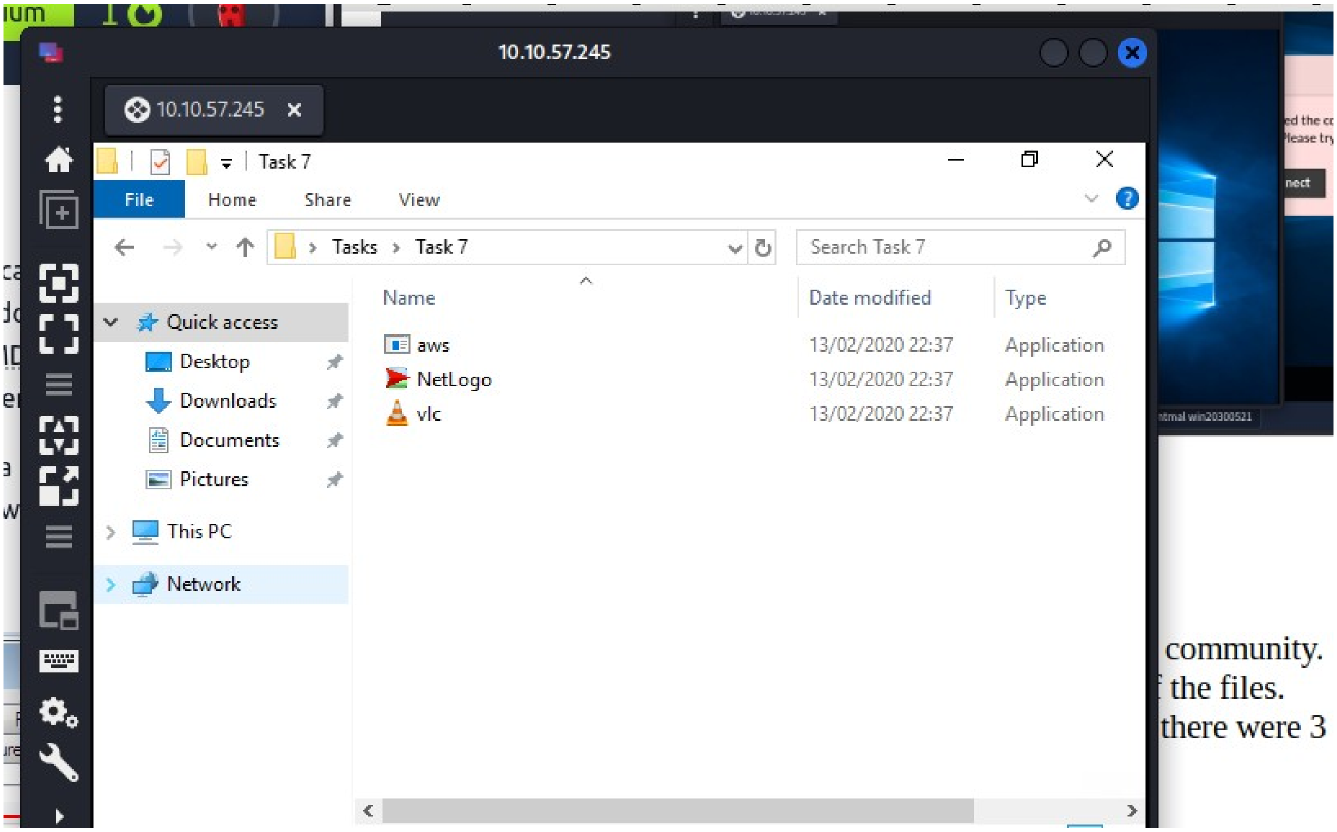


Obtaining md5 checksum of Provided Files

-MD5 checksum are prominent attribute in the malware community.

- These MD5 checksum are cryptographic fingerprints of the files.

- I navigated to the tasks folder then went to task 7 where there were 3 files.

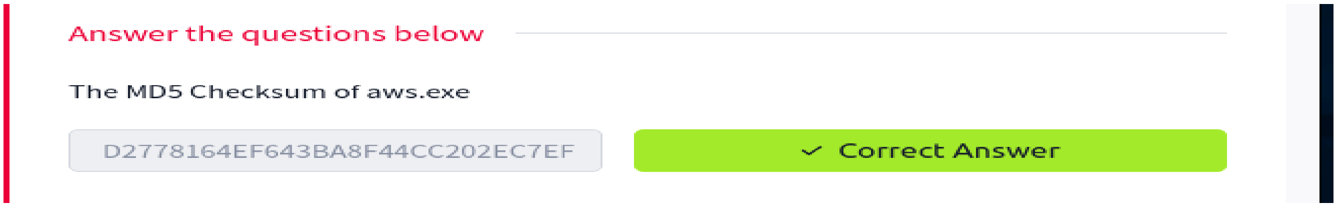


Name	Date modified	Type
aws	13/02/2020 22:37	Application
NetLogo	13/02/2020 22:37	Application
vlc	13/02/2020 22:37	Application

- The vlc app can be a malware that maybe renamed to a vlc app so to confirm we need to check the MD5 checksum
- I used the hash tab to check the checksum

Questions

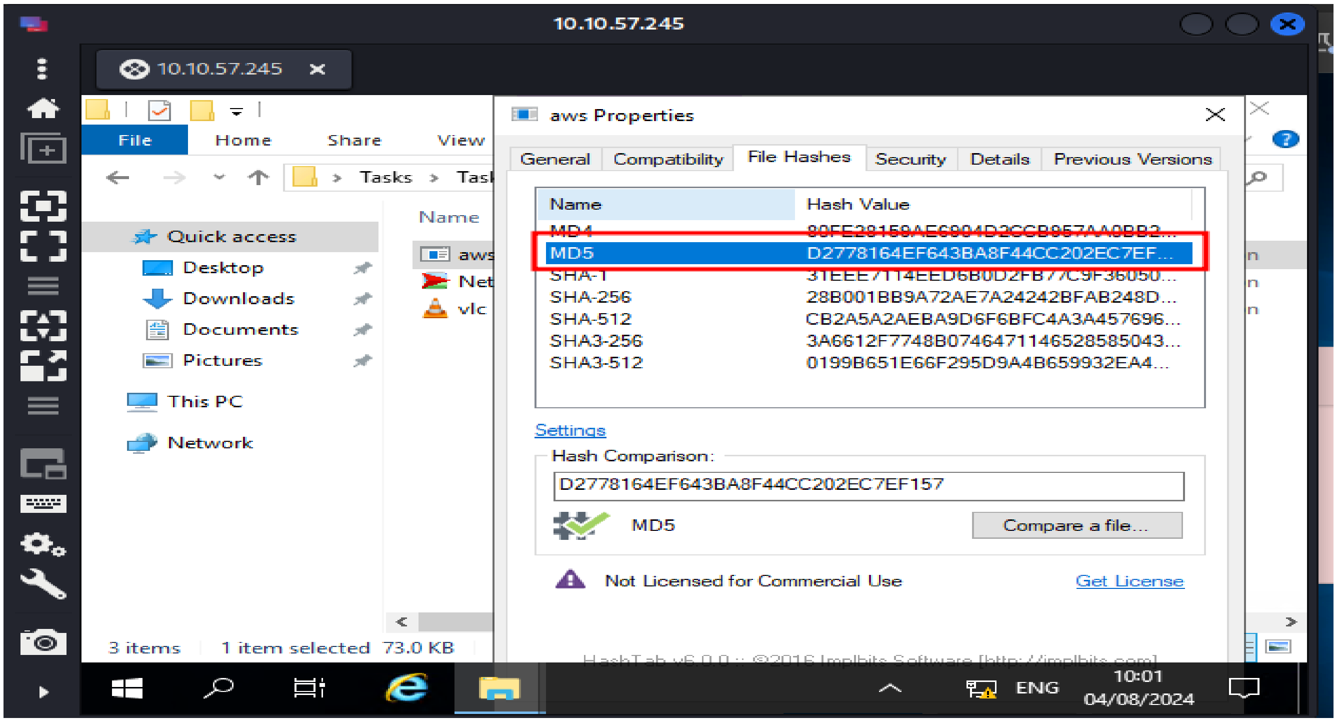
1.



Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202EC7EF



aws Properties

Name	Hash Value
MD4	80FE28159AE6904D2CCB957AA0BB2...
MD5	D2778164EF643BA8F44CC202EC7EF...
SHA-1	31EEE7114EED6B0D2FB77C9F36050...
SHA-256	28B001BB9A72AE7A24242BFAB248D...
SHA-512	CB2A5A2AEBA9D6F6BFC4A3A457696...
SHA3-256	3A6612F7748B0746471146528585043...
SHA3-512	0199B651E66F295D9A4B659932EA4...

Settings

Hash Comparison:

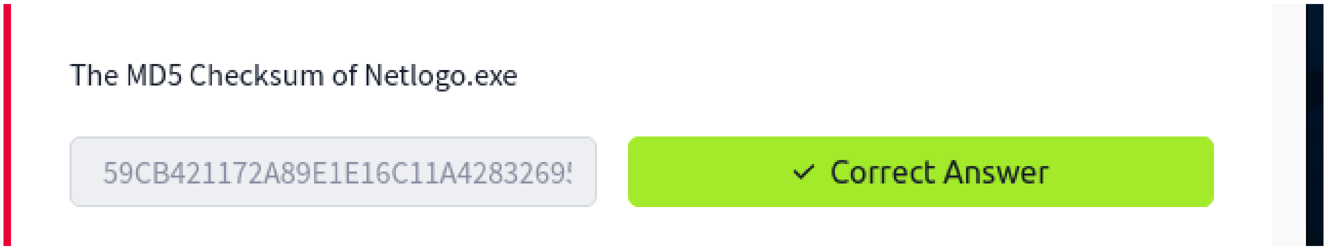
D2778164EF643BA8F44CC202EC7EF157

MD5

Not Licensed for Commercial Use

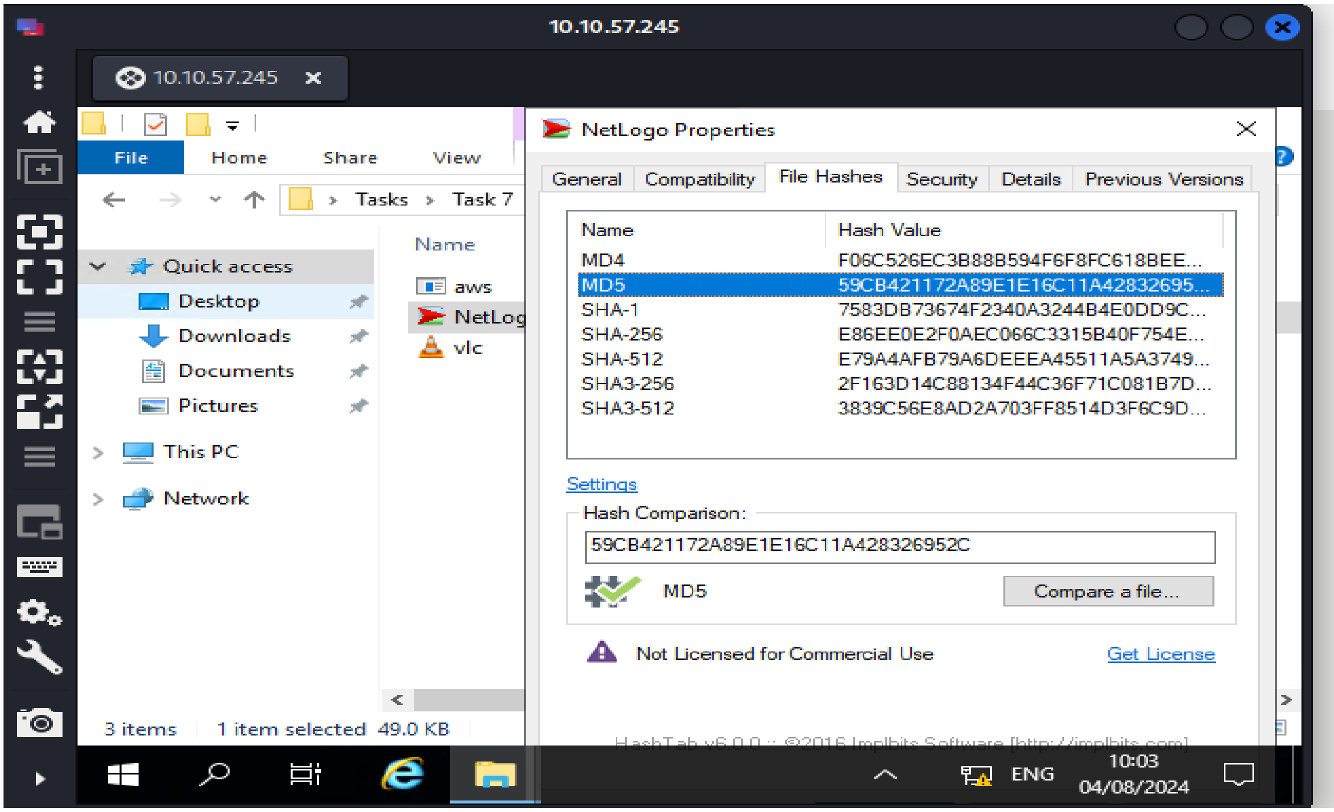
HashTab v6.0.0 :: ©2016 Implbits Software [http://implbits.com]

2.



The MD5 Checksum of Netlogo.exe

59CB421172A89E1E16C11A4283269!



NetLogo Properties

Name	Hash Value
MD4	F06C526EC3B88B594F6F8FC618BEE...
MD5	59CB421172A89E1E16C11A42832695...
SHA-1	7583DB73674F2340A3244B4E0DD9C...
SHA-256	E86EE0E2F0AEC066C3315B40F754E...
SHA-512	E79A4AFB79A6DEEEA45511A5A3749...
SHA3-256	2F163D14C88134F44C36F71C081B7D...
SHA3-512	3839C56E8AD2A703FF8514D3F6C9D...

Settings

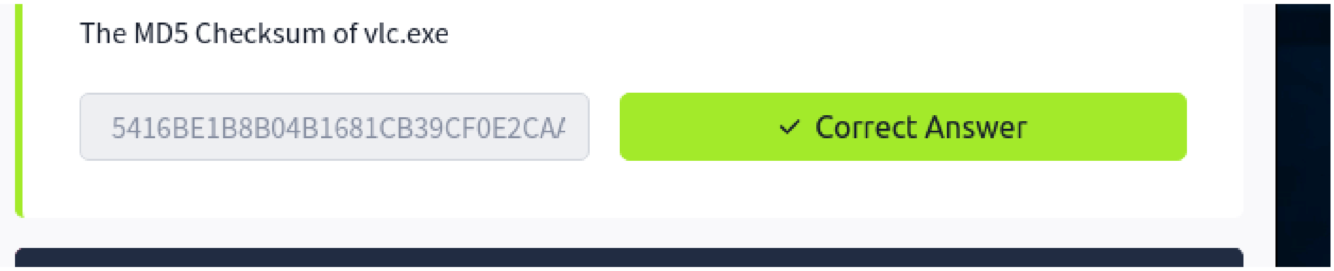
Hash Comparison: 59CB421172A89E1E16C11A428326952C

MD5

Not Licensed for Commercial Use

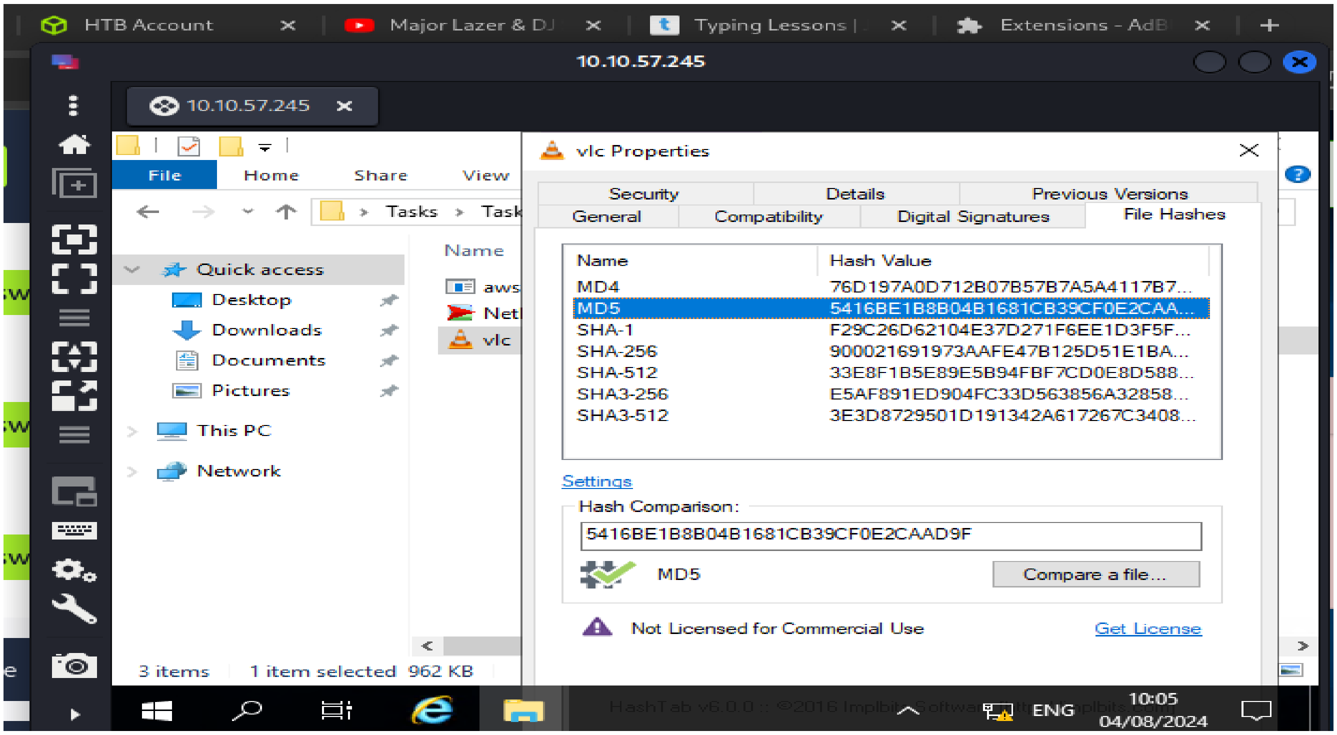
HashTab v6.0.0 :: ©2016 Implbits Software [http://implbits.com]

3.



The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF0E2CA/



vlc Properties

Name	Hash Value
MD4	76D197A0D712B07B57B7A5A4117B7...
MD5	5416BE1B8B04B1681CB39CF0E2CAA...
SHA-1	F29C26D62104E37D271F6EE1D3F5F...
SHA-256	900021691973AAFE47B125D51E1BA...
SHA-512	33E8F1B5E89E5B94FBF7CD0E8D588...
SHA3-256	E5AF891ED904FC33D563856A32858...
SHA3-512	3E3D8729501D191342A617267C3408...

Settings

Hash Comparison:

5416BE1B8B04B1681CB39CF0E2CAAD9F

MD5

Compare a file...

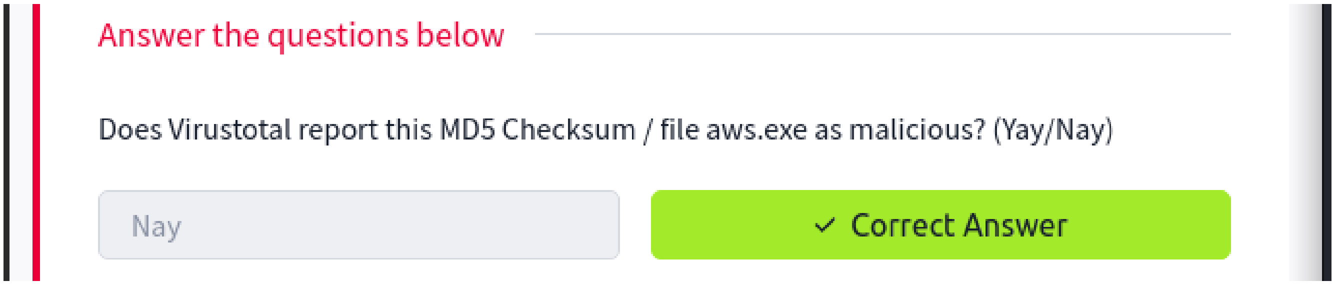
Not Licensed for Commercial Use

Get License

Now lets see if the MD5 checksum have been analyses before

Questions

1.

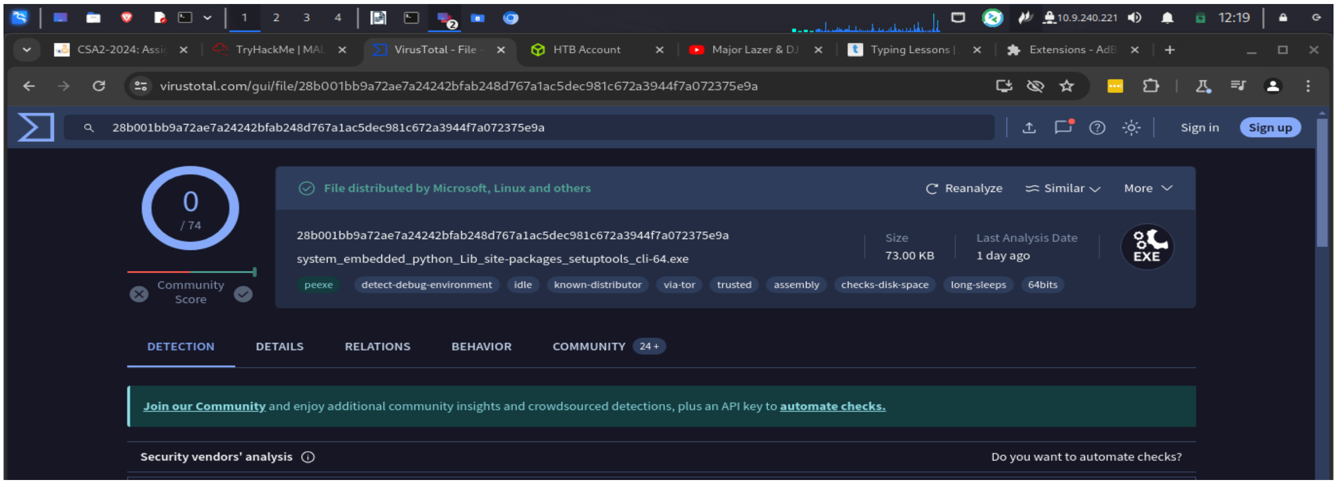


Answer the questions below

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

Nay

✓ Correct Answer



virustotal.com/gui/file/28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a

28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a

0
/ 74

File distributed by Microsoft, Linux and others

28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a

system_embedded_python_Lib_site-packages_setuptools_cli-64.exe

Size 73.00 KB

Last Analysis Date 1 day ago

peexe detect-debug-environment idle known-distributor via-tor trusted assembly checks-disk-space long-sleeps 64bits

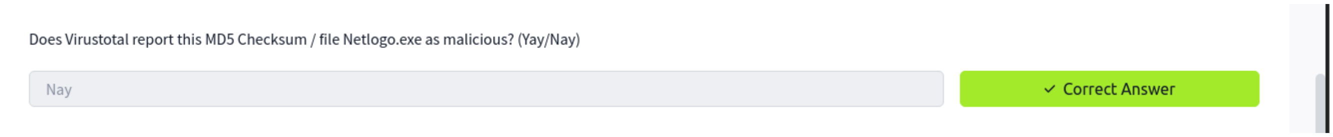
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 24 +

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

Security vendors' analysis

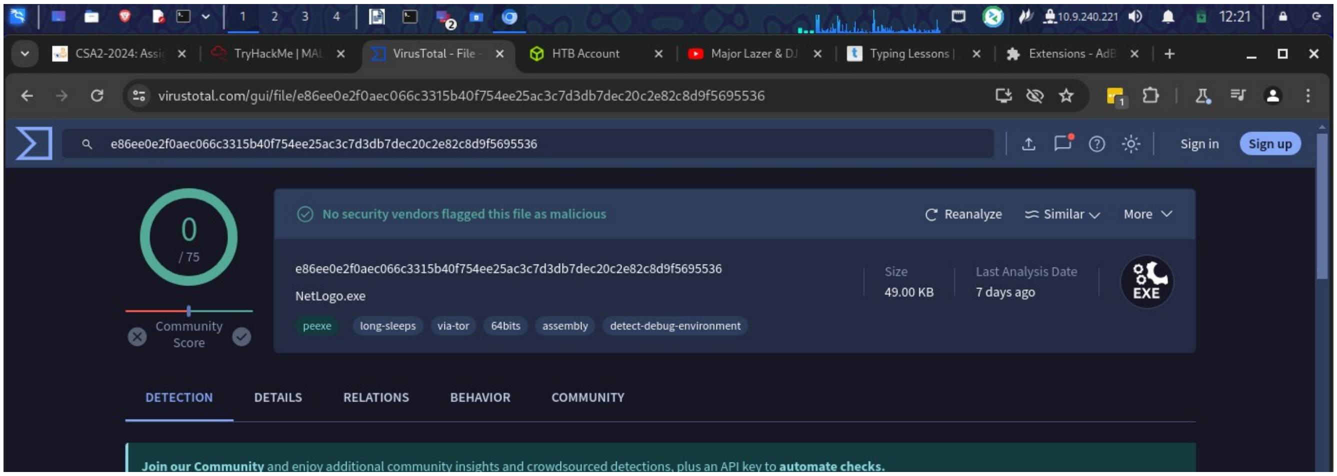
Do you want to automate checks?

2.



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

Nay



virustotal.com/gui/file/e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536

No security vendors flagged this file as malicious

0 / 75

e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536

NetLogo.exe

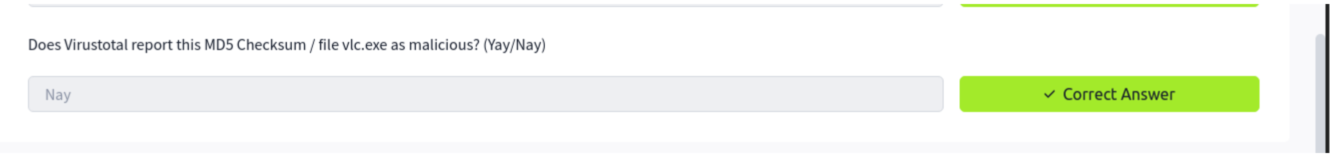
Size 49.00 KB

Last Analysis Date 7 days ago

peexe long-sleeps via-tor 64bits assembly detect-debug-environment

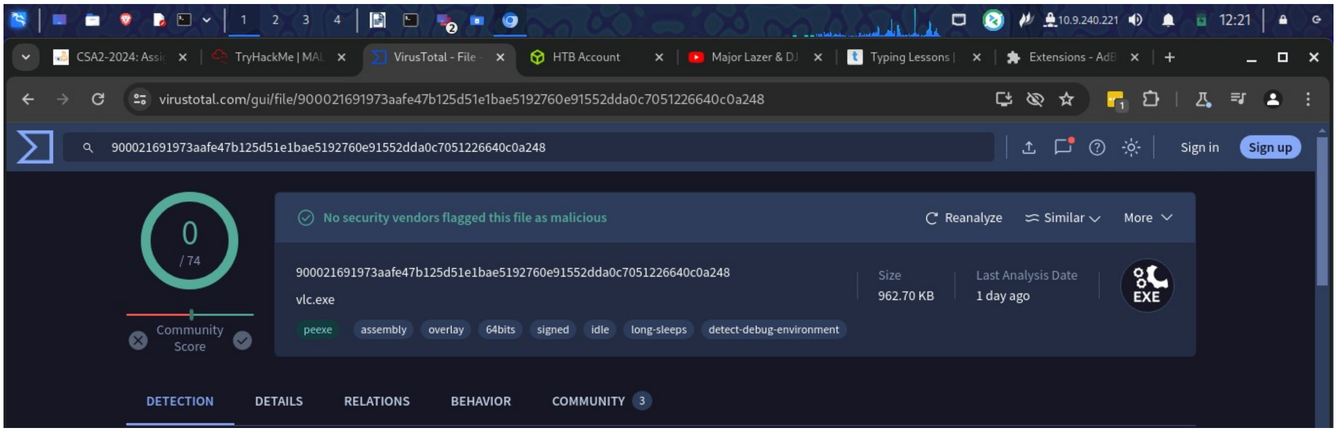
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

3.



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

Nay



virustotal.com/gui/file/900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248

No security vendors flagged this file as malicious

0 / 74

900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248

vlc.exe

Size 962.70 KB

Last Analysis Date 1 day ago

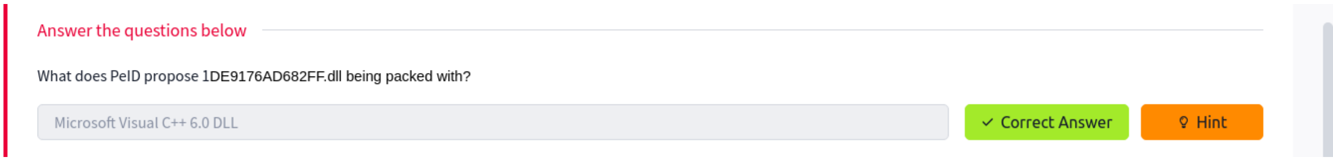
peexe assembly overlay 64bits signed idle long-sleeps detect-debug-environment

Identifying if the executables are obfuscated/packed

- We are going to use PelD which has a huge database.
- A file can be executable even without the “.exe”
- An executable file has a hex value of ‘4D 5A’ so even a jpg file with the same hex value can be executable

Questions

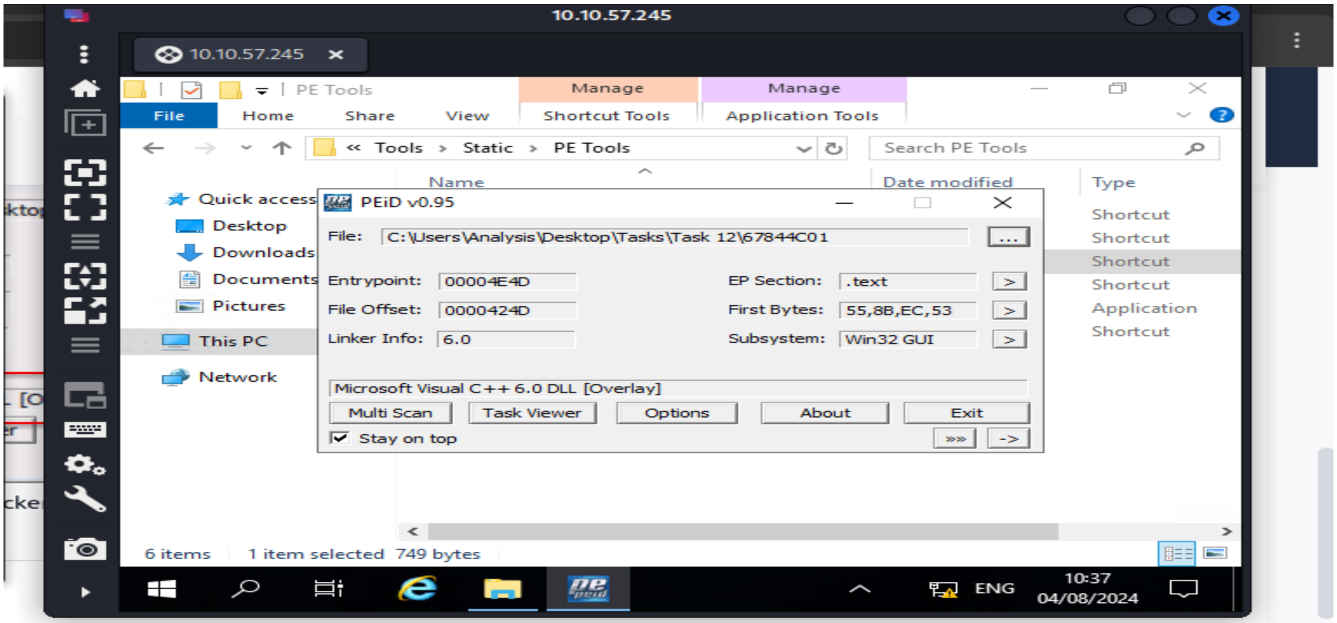
1.



Answer the questions below

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

Microsoft Visual C++ 6.0 DLL



10.10.57.245

PEiD v0.95

File: C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01

Entrypoint: 00004E4D

EP Section: .text

File Offset: 0000424D

First Bytes: 55,8B,EC,53

Linker Info: 6.0

Subsystem: Win32 GUI

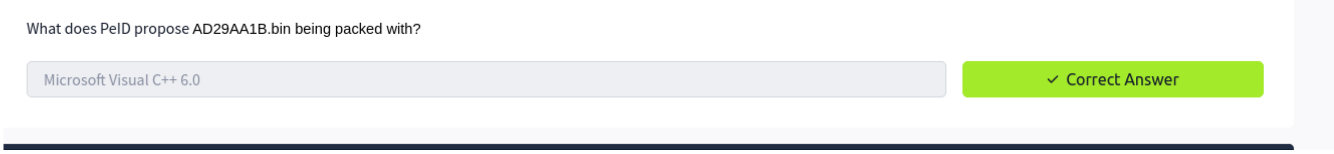
Microsoft Visual C++ 6.0 DLL [Overlay]

☑ Stay on top

6 items 1 item selected 749 bytes

10:37 04/08/2024

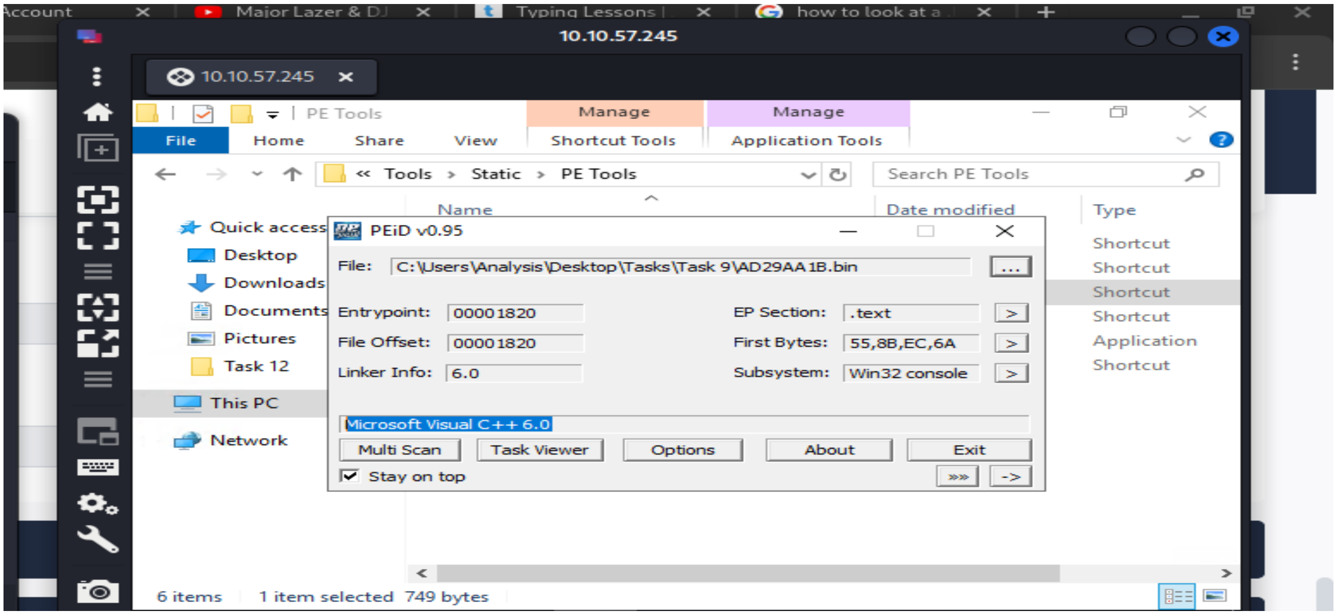
2.



What does PeID propose AD29AA1B.bin being packed with?

Microsoft Visual C++ 6.0

For this I had to look for the file and I found it in task 9. I used PeiD which was in the tools folder.



10.10.57.245

PEiD v0.95

File: C:\Users\Analysis\Desktop\Tasks\Task 9\AD29AA1B.bin

Entrypoint: 00001820

EP Section: .text

File Offset: 00001820

First Bytes: 55,8B,EC,6A

Linker Info: 6.0

Subsystem: Win32 console

Microsoft Visual C++ 6.0

☑ Stay on top

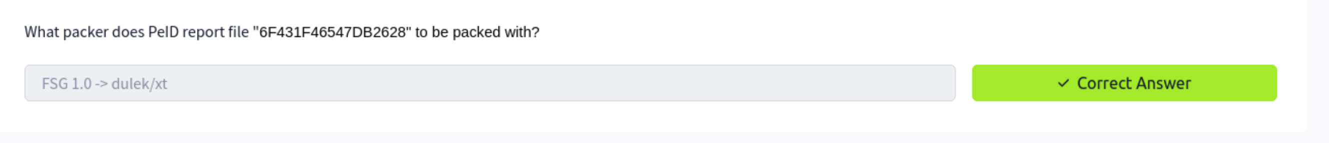
6 items 1 item selected 749 bytes

What is Obfuscation/packing

- Packing is a form of obfuscation that malware authors use to prevent analysis of programmes
- For legitimate reasons it is used for protection of intellectual property
- On the other hand it is done to prevent the malware analyst to reverse it so that they can not know the behavior of the malware.

Questions

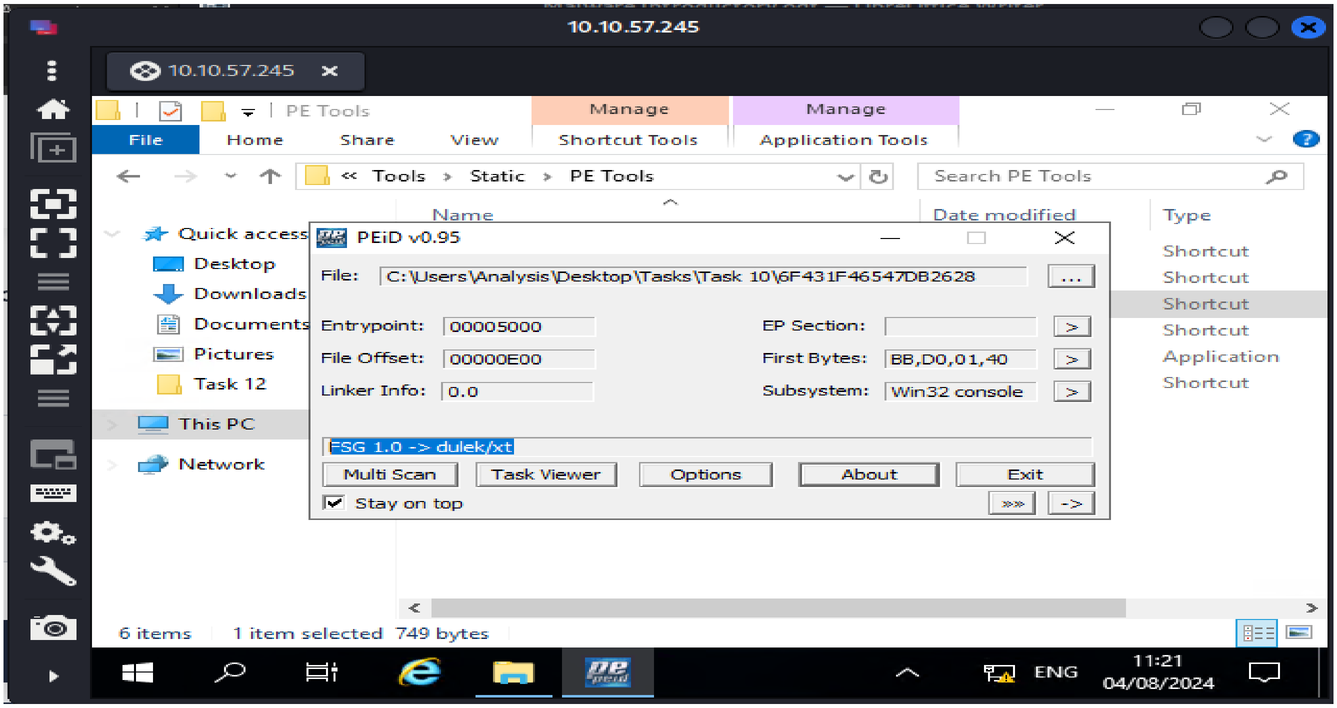
1.



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

FSG 1.0 -> dulek/xt

✓ Correct Answer



File: C:\Users\Analysis\Desktop\Tasks\Task 10\6F431F46547DB2628

Entrypoint: 00005000

EP Section:

File Offset: 00000E00

First Bytes: BB,D0,01,40

Linker Info: 0.0

Subsystem: Win32 console

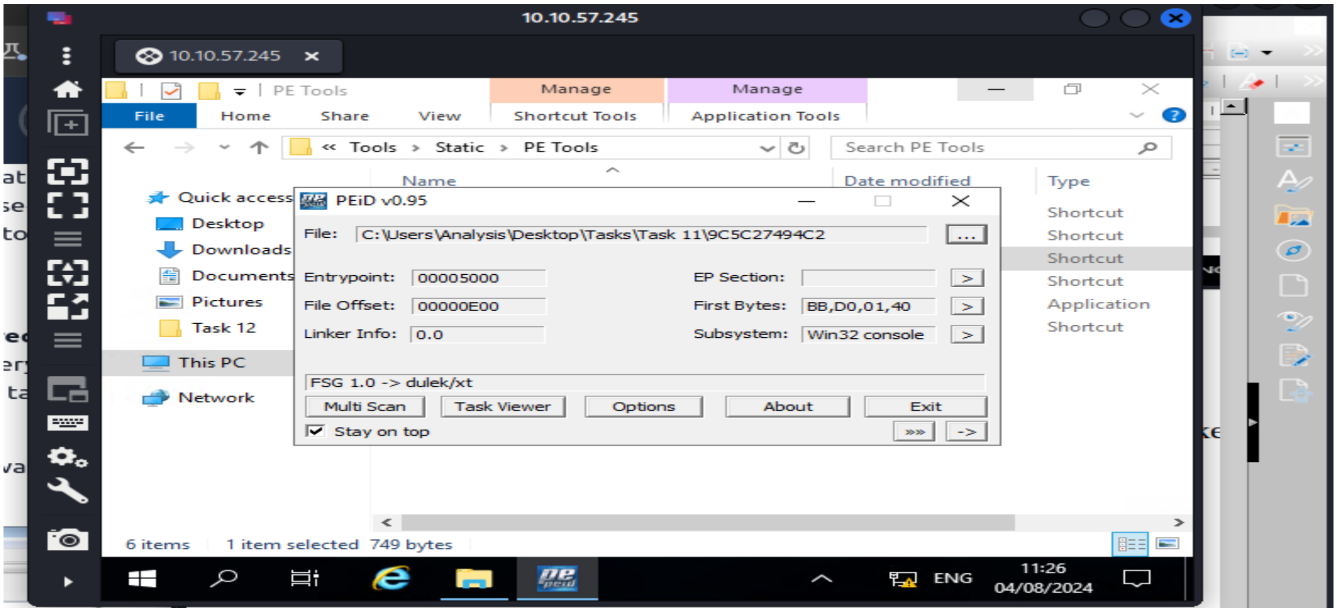
FSG 1.0 -> dulek/xt

☑ Stay on top

6 items 1 item selected 749 bytes

Visualizing the differences between packed and non-packed code

- Whilst the PeiD has a large database. It does not have every packer.
- So we navigate to task 11 where the PeiD was able to detect the packer being used bit it was not able to de-obfuscate them



PEiD v0.95

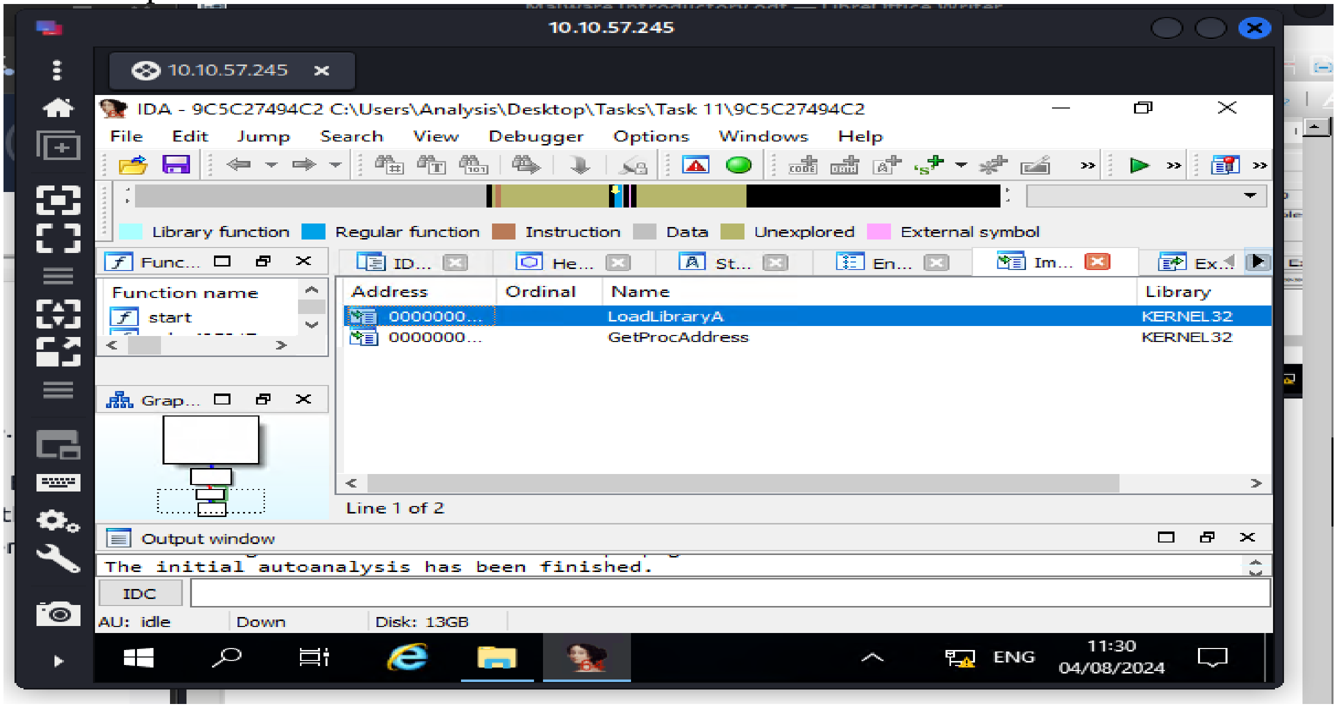
File: C:\Users\Analysis\Desktop\Tasks\Task 11\9C5C27494C2

Entrypoint:	00005000	EP Section:	
File Offset:	00000E00	First Bytes:	BB,D0,01,40
Linker Info:	0.0	Subsystem:	Win32 console

FSG 1.0 -> dulek/xt

☑ Stay on top

- So we open the file with a tool called IDA freeware.



IDA - 9C5C27494C2 C:\Users\Analysis\Desktop\Tasks\Task 11\9C5C27494C2

Address	Ordinal	Name	Library
0000000...		LoadLibraryA	KERNEL32
0000000...		GetProcAddress	KERNEL32

Line 1 of 2

Output window

```
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 13GB

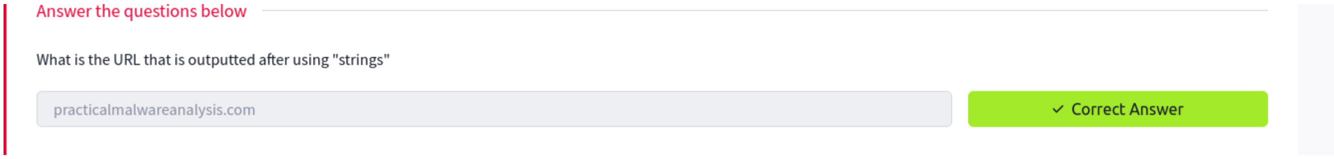
- Two imports were noted
- We also had a flow of how the programs executed
-

Introduction to strings

- Strings are the ASCII/text contents of a programs
- In this section I was to open file Sysinternalssuite in the command prompt

Questions

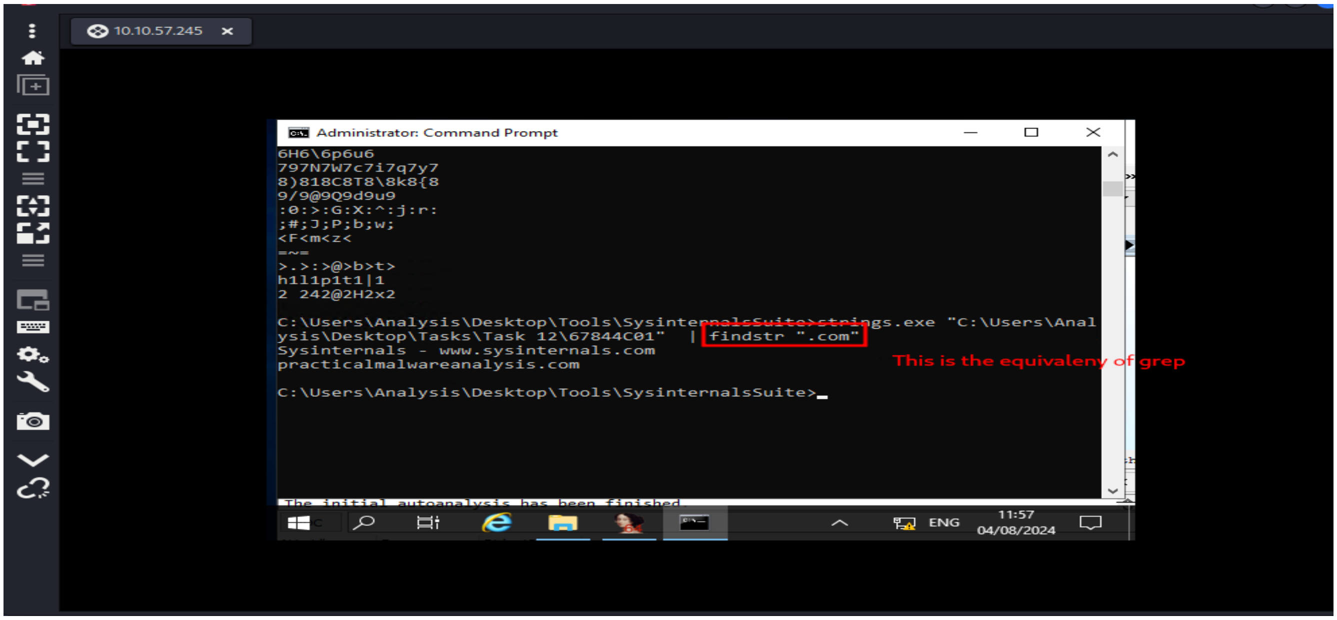
1.



Answer the questions below

What is the URL that is outputted after using "strings"

practicalmalwareanalysis.com

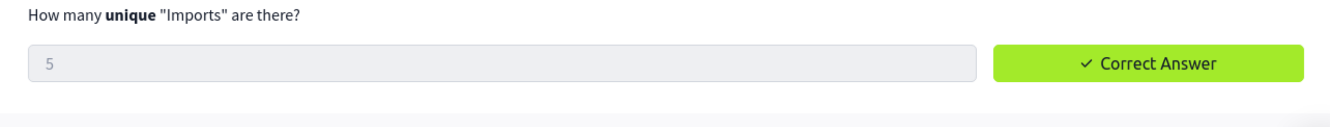


```
6H6\6p6u6
797N7W7c7i7q7y7
8)818C8T8\8k8{8
9/9@9Q9d9u9
:0:>:G:X:^:j:r:
;#;J;P;b;w;
<F<m<z<
=~=
>.>:>@>b>t>
h1l1p1t1|1
2 242@2H2x2

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>strings.exe "C:\Users\Anal
ysis\Desktop\Tasks\Task 12\67844C01"  | findstr ".com"
Sysinternals - www.sysinternals.com
practicalmalwareanalysis.com

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>_
```

This is the equivaleny of grep

The initial autoanalysis has been finished.

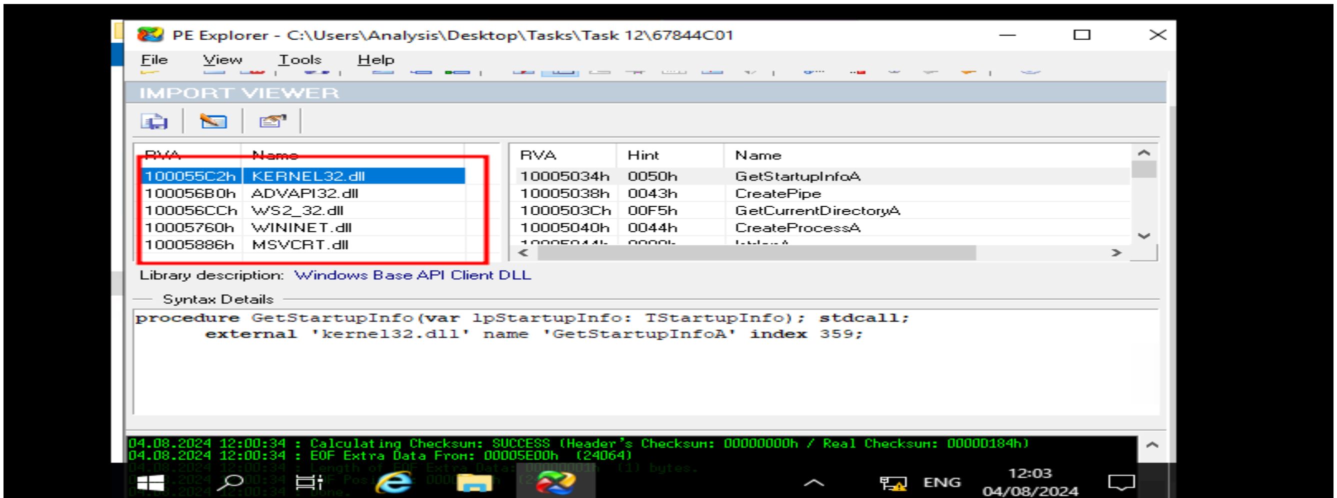
2.



How many **unique** "Imports" are there?

5

For this I had to open the PE Explorer and dropped the file there. I then navigated to the view tab where there was an option for imports



PE Explorer - C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01
File
View
Tools
Help
IMPORT VIEWER

RVA	Name
100055C2h	KERNEL32.dll
100056B0h	ADVAPI32.dll
100056CCh	WS2_32.dll
10005760h	WININET.dll
10005886h	MSVCRT.dll

RVA	Hint	Name
10005034h	0050h	GetStartupInfoA
10005038h	0043h	CreatePipe
1000503Ch	00F5h	GetCurrentDirectoryA
10005040h	0044h	CreateProcessA

Library description: Windows Base API Client DLL

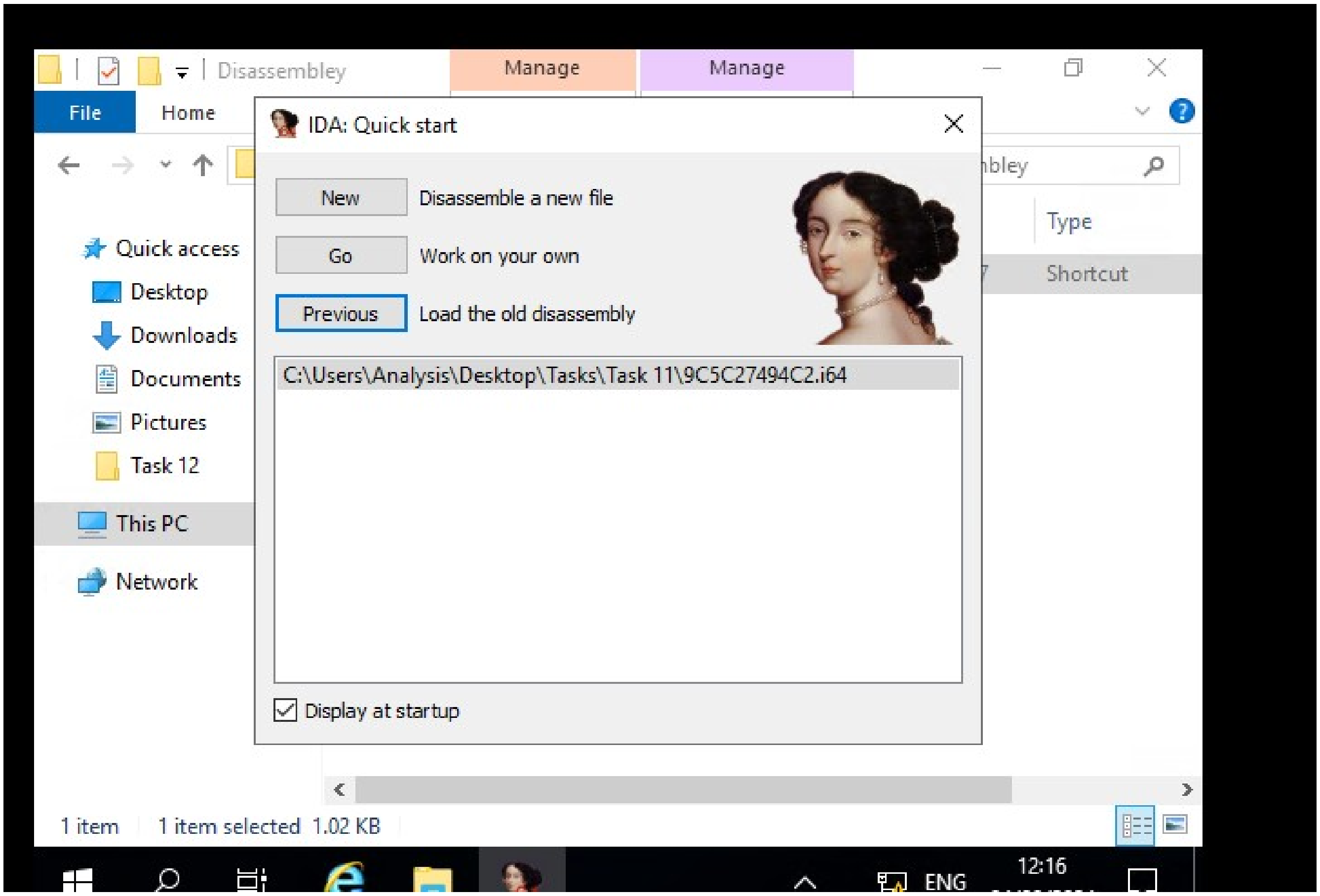
Syntax Details

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

```
04.08.2024 12:00:34 : Calculating Checksum: SUCCESS (Header's Checksum: 00000000h / Real Checksum: 00000184h)
04.08.2024 12:00:34 : EOF Extra Data From: 00005E00h  (24064)
```

Introduction to imports

- IDA Freeware is a tool that can be used for both dynamic and static analysis
- Disassemblers reverse the complied code of a program from machine code to human-readable.
- Debuggers works the same but it can view the changes made throughout each step
- To use we first launch the IDA Freeware and select import

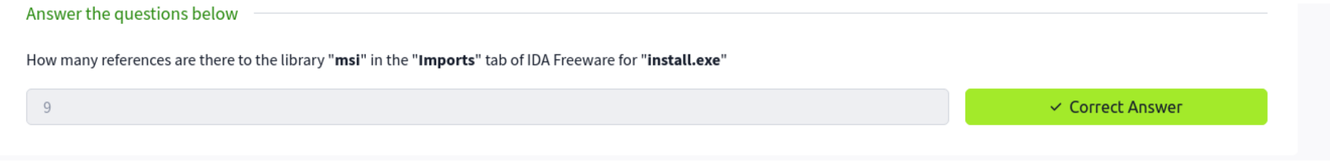


C:\Users\Analysis\Desktop\Tasks\Task 11\9C5C27494C2.i64

- then I chose the file install.exe located at task 13
- Then you navigate to the view tab which contains the import options

Questions

1.

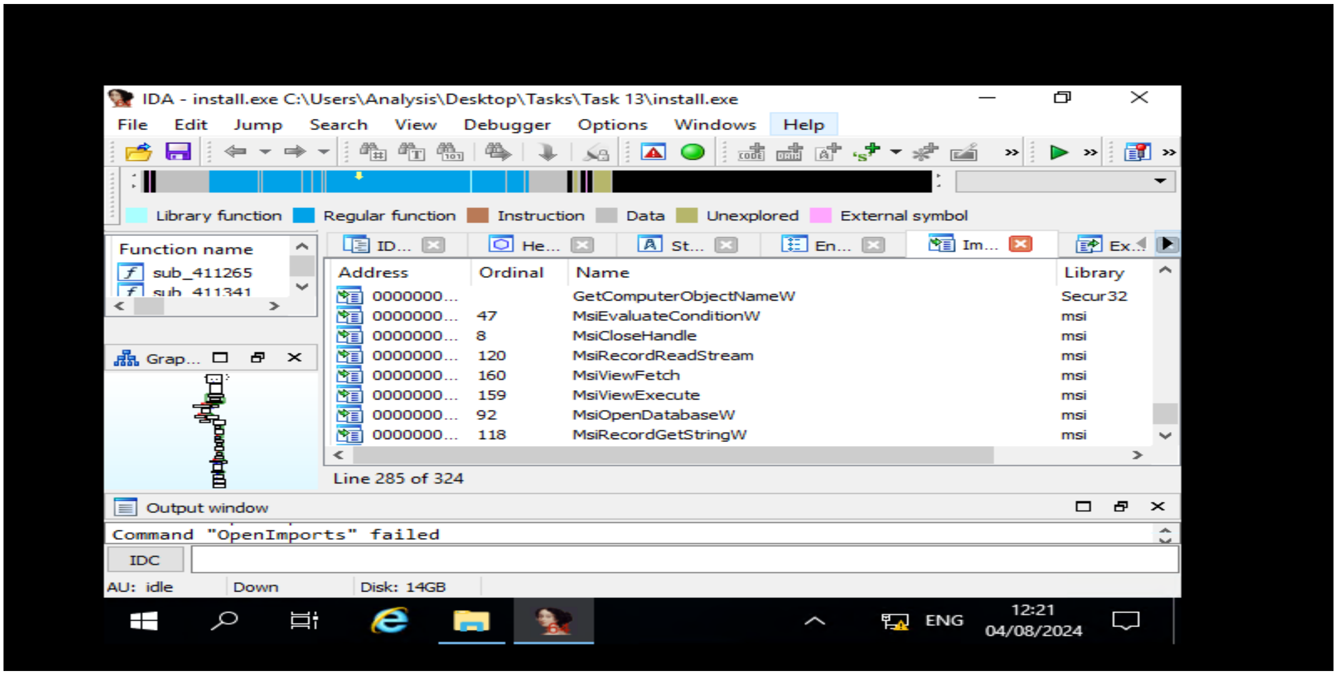


Answer the questions below

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

9

✓ Correct Answer



IDA - install.exe C:\Users\Analysis\Desktop\Tasks\Task 13\install.exe

File Edit Jump Search View Debugger Options Windows Help
Library function Regular function Instruction Data Unexplored External symbol
Function name
sub_411265
sub_411341
Grap...
ID... He... St... En... Im... Ex...

Address	Ordinal	Name	Library
0000000...		GetComputerObjectNameW	Secur32
0000000...	47	MsiEvaluateConditionW	msi
0000000...	8	MsiCloseHandle	msi
0000000...	120	MsiRecordReadStream	msi
0000000...	160	MsiViewFetch	msi
0000000...	159	MsiViewExecute	msi
0000000...	92	MsiOpenDatabaseW	msi
0000000...	118	MsiRecordGetStringW	msi

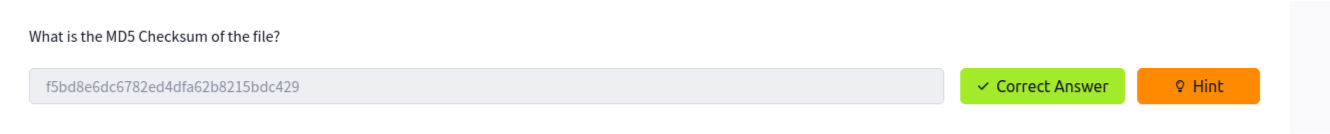
Line 285 of 324

Output window

```
Command "OpenImports" failed
```

Practical Summary

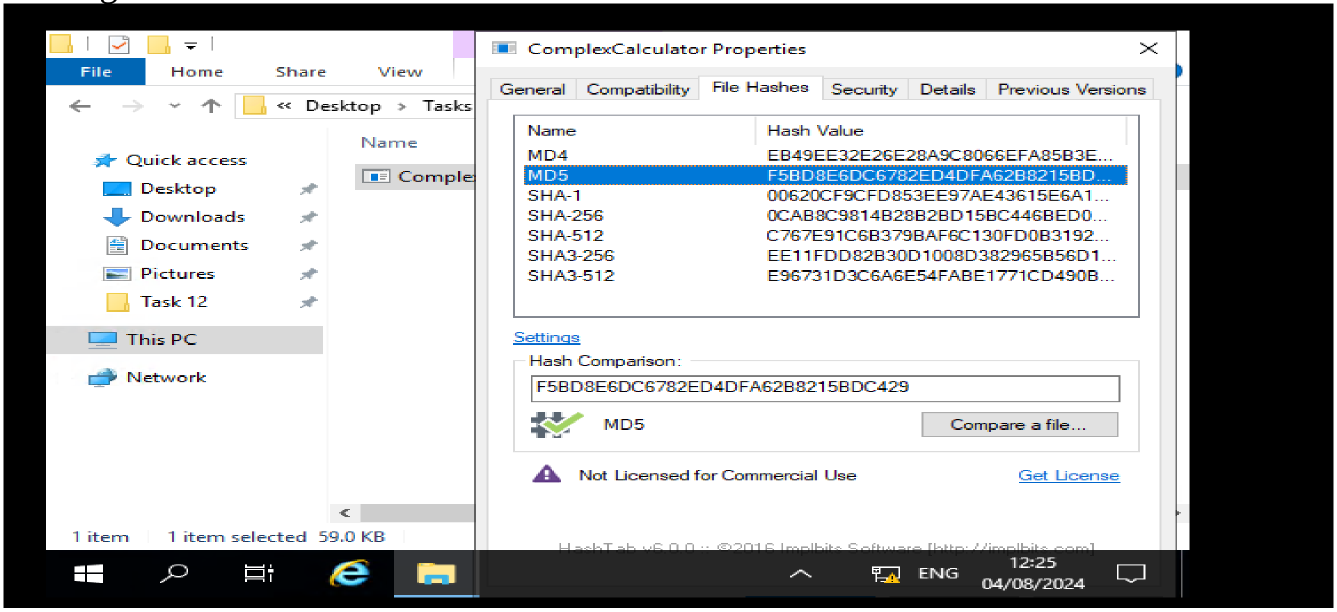
1.



What is the MD5 Checksum of the file?

f5bd8e6dc6782ed4dfa62b8215bdc429

For this I used the Hash Tab which can be accessed by right clicking on the file then moving to file hashes



ComplexCalculator Properties

Name	Hash Value
MD4	EB49EE32E26E28A9C8066EFA85B3E...
MD5	F5BD8E6DC6782ED4DFA62B8215BD...
SHA-1	00620CF9CFD853EE97AE43615E6A1...
SHA-256	0CAB8C9814B28B2BD15BC446BED0...
SHA-512	C767E91C6B379BAF6C130FD0B3192...
SHA3-256	EE11FDD82B30D1008D382965B56D1...
SHA3-512	E96731D3C6A6E54FABE1771CD490B...

Settings

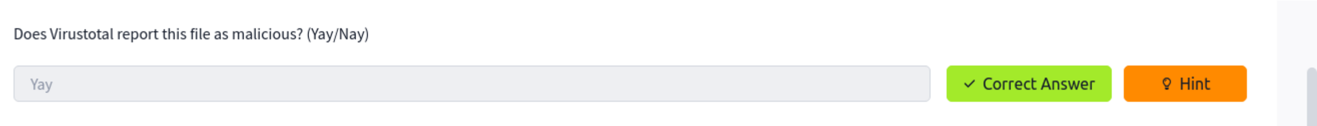
Hash Comparison:

F5BD8E6DC6782ED4DFA62B8215BDC429

MD5

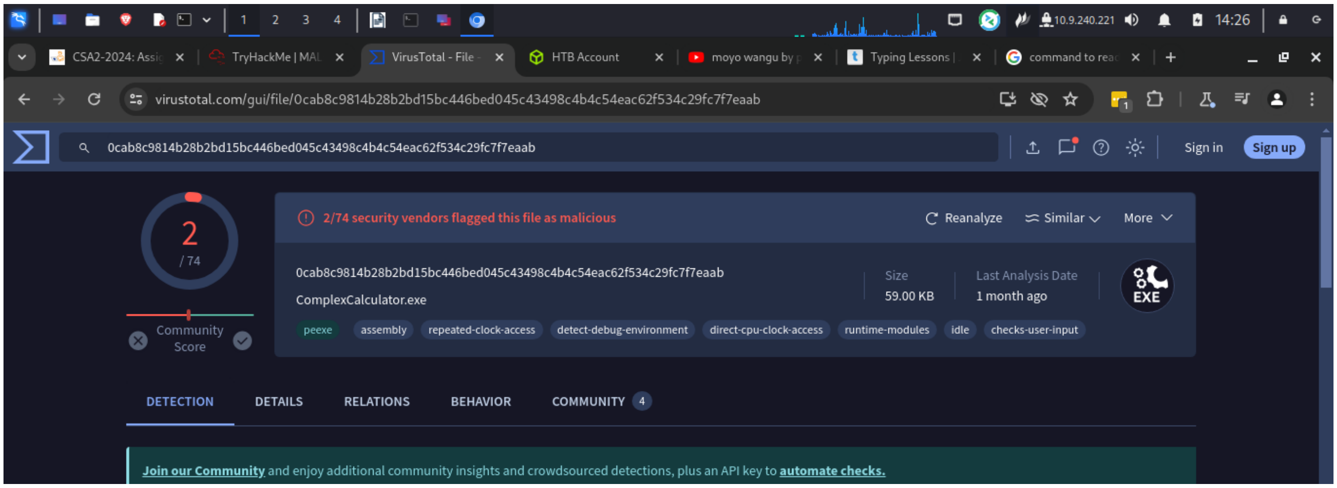
Compare a file...
Not Licensed for Commercial Use
Get License
HashTab v6.0.0 :: ©2016 Implbits Software [http://implbits.com]
ENG 12:25 04/08/2024

2.



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

Yay



virustotal.com/gui/file/0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

2 / 74

2/74 security vendors flagged this file as malicious

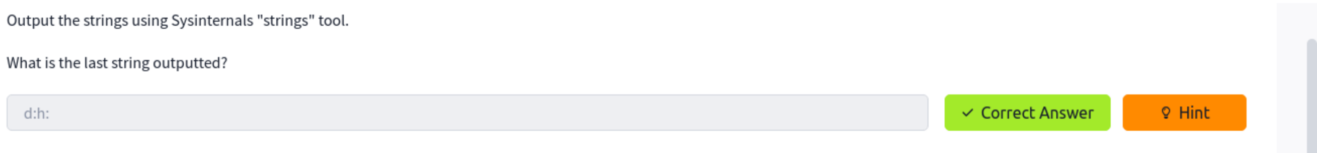
0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab
ComplexCalculator.exe

Size: 59.00 KB
Last Analysis Date: 1 month ago

peexe assembly repeated-clock-access detect-debug-environment direct-cpu-clock-access runtime-modules idle checks-user-input

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

3.

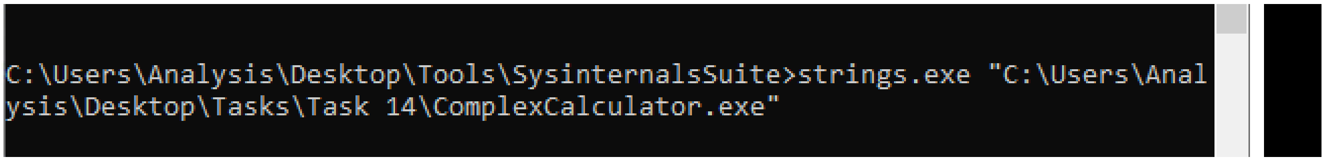


Output the strings using Sysinternals "strings" tool.

What is the last string outputted?

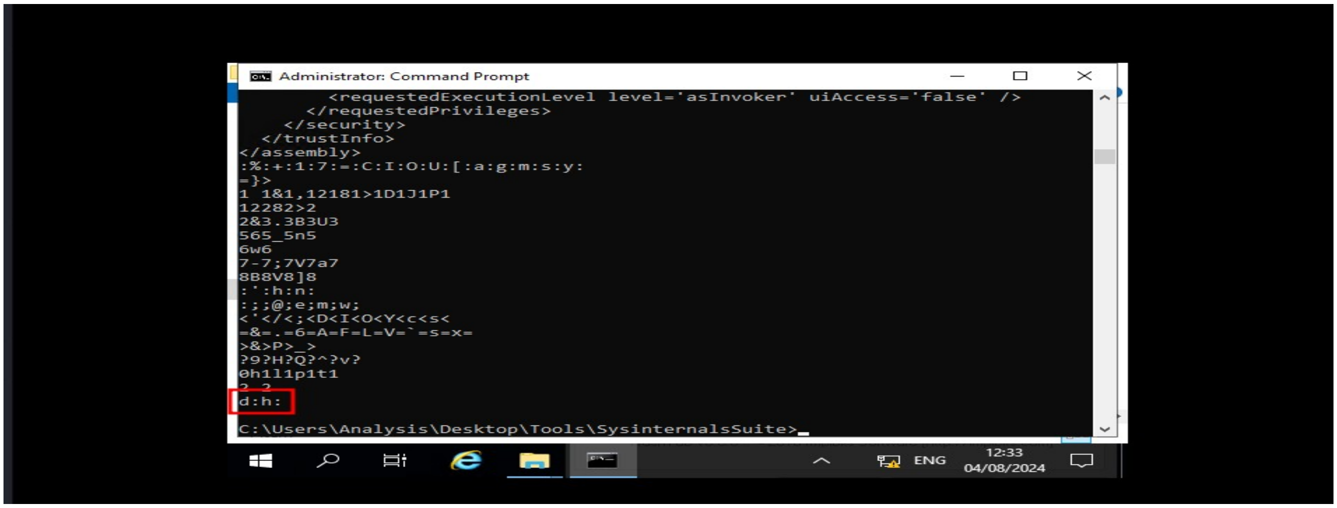
d:h:

I used the command prompt
Here is the command



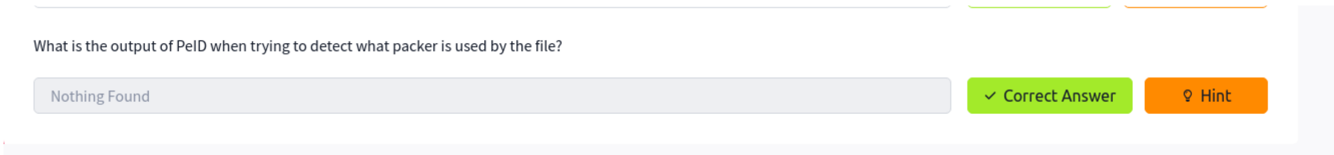
```
C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>strings.exe "C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculator.exe"
```

And here is the answer



```
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
:%:+:1:7:=:C:I:O:U:[:a:g:m:s:y:
=}>
1 1&1,12181>1D1J1P1
12282>2
2&3.3B3U3
565_5n5
6w6
7-7;7V7a7
8B8V8]8
:':h:n:
:;;@;e;m;w;
<'</<;<D<I<O<Y<c<s<
=&=.=6=A=F=L=V=`=s=x=
>&>P>_>
?9?H?Q?^?v?
0h1l1p1t1
2 2
d:h:

C:\Users\Analysis\Desktop\Tools\SysinternalsSuite>_
```

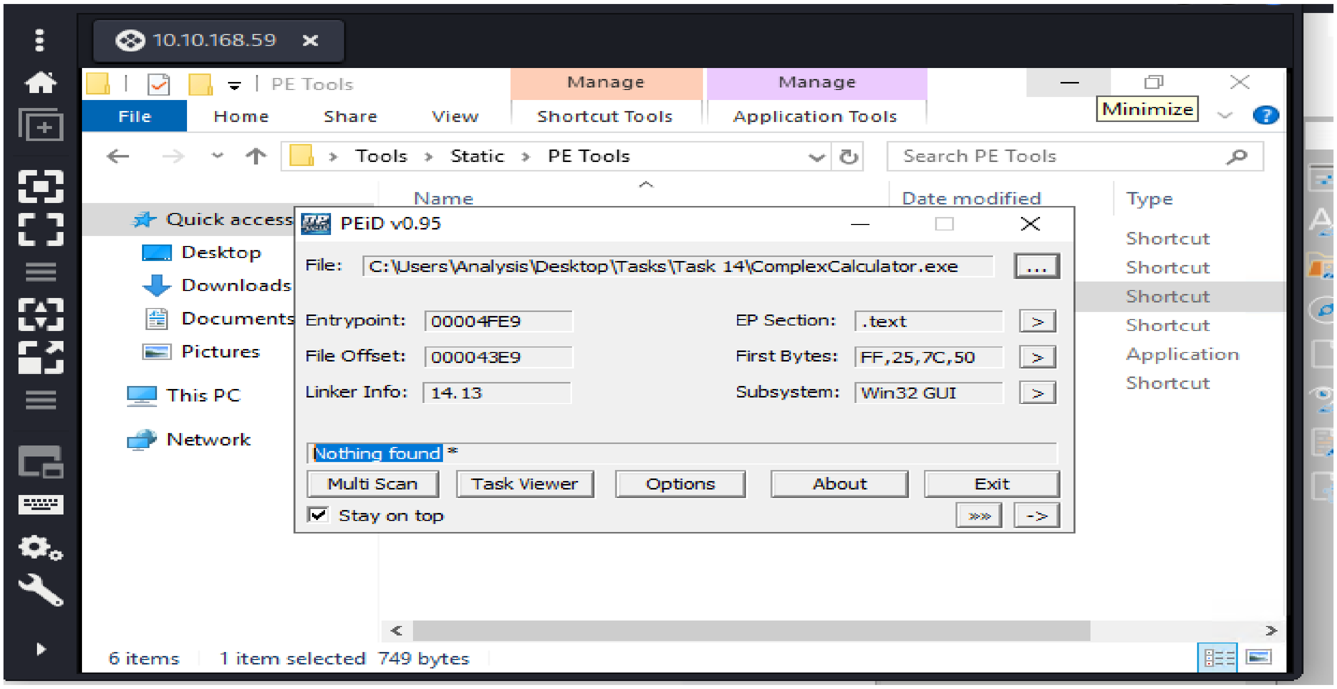
4.



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

Nothing Found

I used the PeiD tool for this



PEiD v0.95

File: C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculator.exe

Entrypoint: 00004FE9

EP Section: .text

File Offset: 000043E9

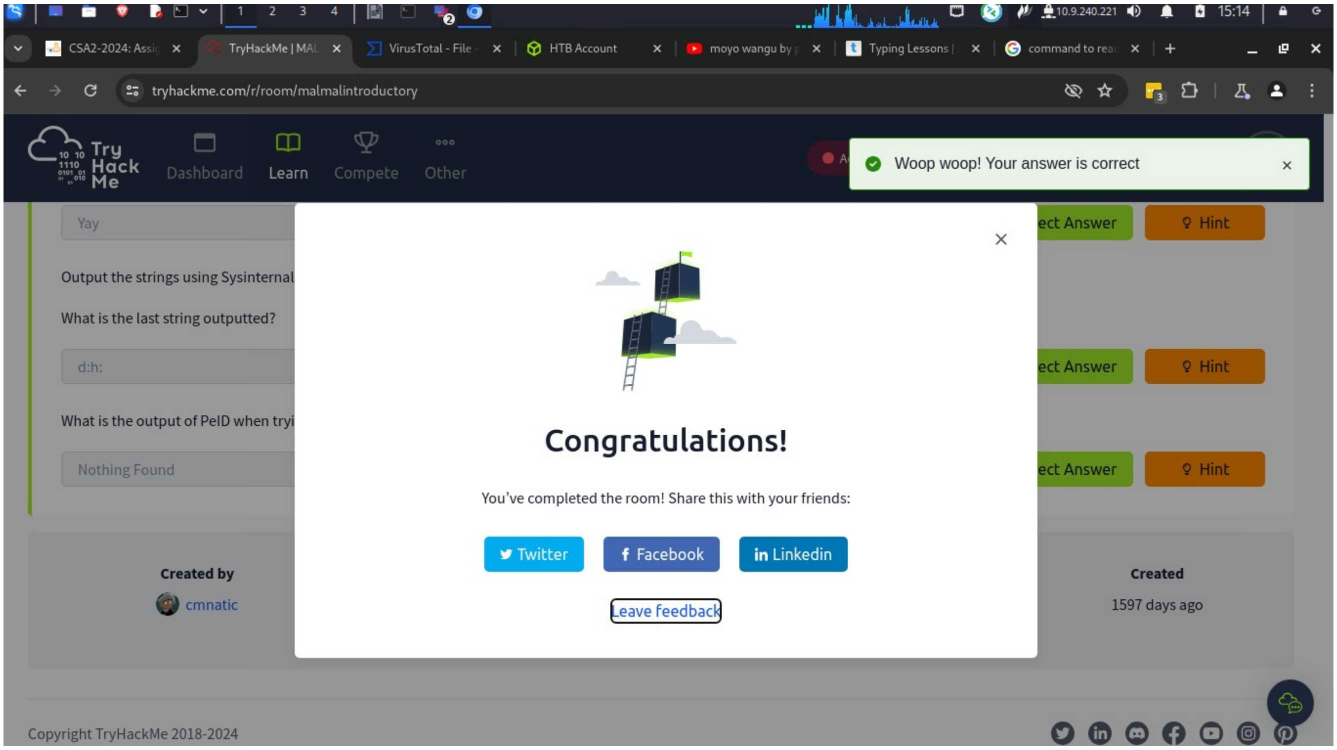
First Bytes: FF,25,7C,50

Linker Info: 14.13

Subsystem: Win32 GUI

Nothing found *

☑ Stay on top



Woop woop! Your answer is correct

Output the strings using Sysinternal

What is the last string outputted?

d:h:

What is the output of PeID when tryi

Nothing Found

Congratulations!

You've completed the room! Share this with your friends:

Created by cmnatic

Created 1597 days ago

Copyright TryHackMe 2018-2024

conclusion

In this room I was able to learn about the MD5 checksum which comes in handy when dealing with Malware. I also went through some the tools that can be used when analyzing a malware. It was a very interesting room.