

Martin Mwangi Njoroge
mwangimartins650@gmail.com

CS-SA08-24031

MAL: Malware Introductory

Here's a link to my finished room,

<https://tryhackme.com/r/room/malmalintroductory>

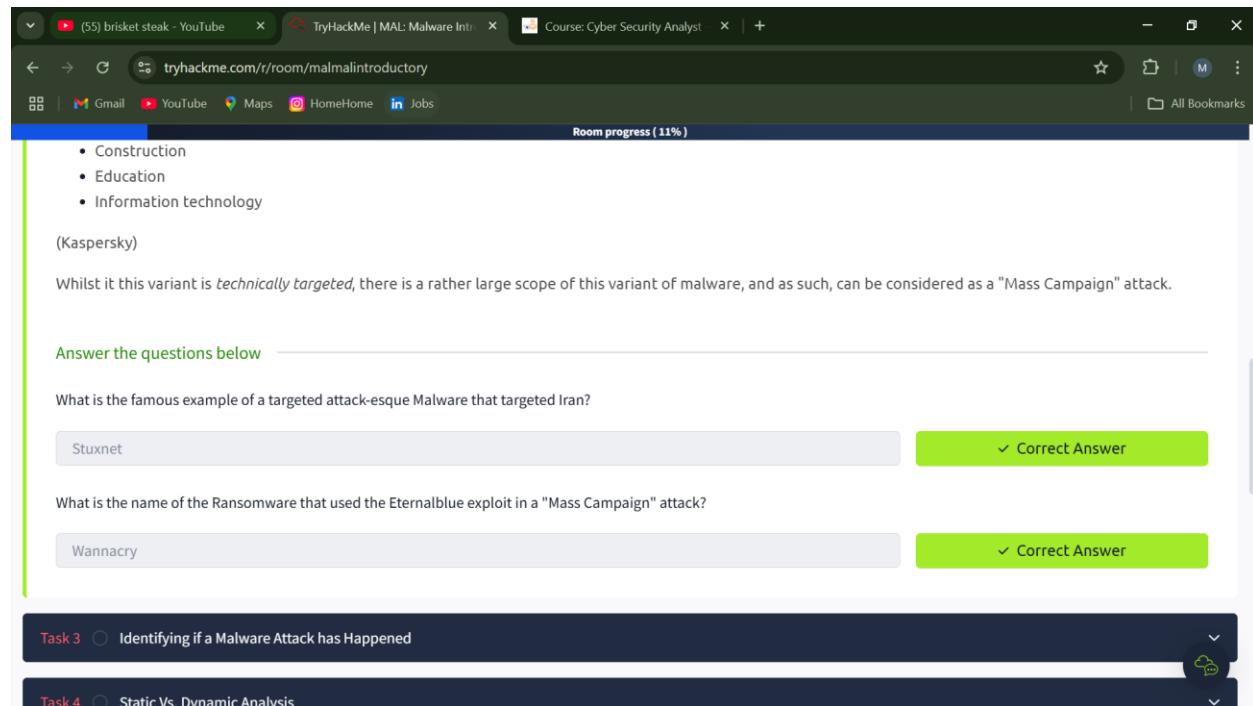
1.0 Introduction

This room focuses on introduction to the techniques and tools used throughout malware analysis. As malware analysis a form of incidence response, and useful in understanding how the behaviors of variants of malware result in their respective categorization.

When analyzing malware, it is important to consider the following; Point of Entry (PoE), indicators that malware has even been executed on a machine, how does the malware perform, can we ultimately prevent and/or detect further infection.

Malware attacks can be categorized as either targeted or mass campaigns.

Questions



Room progress (11%)

- Construction
- Education
- Information technology

(Kaspersky)

Whilst it this variant is *technically targeted*, there is a rather large scope of this variant of malware, and as such, can be considered as a "Mass Campaign" attack.

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

Task 3 Identifying if a Malware Attack has Happened

Task 4 Static Vs. Dynamic Analysis

1.1 Identifying if a Malware Attack has Happened

Malware leaves quite an extensive paper trail of evidence, that we can use to conduct an analysis.

Malware attack can be broken down into a few broad steps, delivery, execution, maintaining persistence, propagation.

These steps will generate lots of network traffic such as communicating with hosts, file system interaction like read/writes and modification.

Fingerprints left behind by a malware attack can be host-based signatures (These are generally speaking the results of execution and any persistence performed by the Malware.) and Network-based signatures.

Questions

The screenshot shows a web browser window with multiple tabs open. The active tab is 'tryhackme.com/r/room/malmalintroductory'. The browser's address bar shows the same URL. The page content is a challenge room with a progress bar at the top indicating 'Room progress (25%)'. There are four questions listed:

- Name the first essential step of a Malware Attack?** The answer 'Delivery' is highlighted in a grey box, and a green button next to it says '✓ Correct Answer'.
- Now name the second essential step of a Malware Attack?** The answer 'Execution' is highlighted in a grey box, and a green button next to it says '✓ Correct Answer'.
- What type of signature is used to classify remnants of infection on a host?** The answer 'Host-Based Signatures' is highlighted in a grey box, and a green button next to it says '✓ Correct Answer'. To its right is an orange button labeled '💡 Hint'.
- What is the name of the other classification of signature used after a Malware attack?** The answer 'Network-Based Signatures' is highlighted in a grey box, and a green button next to it says '✓ Correct Answer'. To its right is an orange button labeled '💡 Hint'.

At the bottom of the challenge room, there is a dark footer bar with the text 'Task 4' and 'Static Vs. Dynamic Analysis'.

1.3 Static Vs. Dynamic Analysis

We can analyze a Malware either by static or dynamic analysis.

With static analysis is used to gain a high-level abstraction of the sample, and with dynamic analysis is a lot more involved, and is where the abstraction of the sample is largely built upon and it essentially involves executing the sample and observing what happens.

1.4 Obtaining MD5 Checksums of Provided Files

Questions

I opened the files properties and then investigated its file hashes where I found the md5 hash

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

Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202 ✓ Correct Answer

The MD5 Checksum of Netlogo.exe

Answer format: ***** Submit

The MD5 Checksum of vlc.exe

Answer format: ***** Submit

Task 8 Now lets see if the MD5 Checksums have been analysed before

File Hashes

Name	Hash Value
MD4	89F2E015A45594B222D8571A3B882...
MD5	D2778164EF643BA8F44CC202ECE7EF...
SHA-1	31EE7114ED9B02D787C936050...
SHA-256	2B8011B85A72AE7A34242BF8A284B...
SHA-512	CB24543A8B43D0F68FC4A3A45796...
SHA3-256	346612F774B074647114652858043...
SHA3-512	01998651E66F295D94AB65932E4...

I opened the files properties and then investigated its file hashes where I found the md5 hash

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

Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202 ✓ Correct Answer

The MD5 Checksum of NetLogo.exe

59CB421172A89E1E16C11A42 ✓ Correct Answer

The MD5 Checksum of vlc.exe

Answer format: ***** Submit

Task 8 Now lets see if the MD5 Checksums have been analysed before

File Hashes

Name	Hash Value
MD4	F0623325D8088554F89FC4110BE...
MD5	E6926E9C2910AC6C96C3315B40F754...
SHA-1	7850B7878747230A3244B4E6D90...
SHA-256	B869E6E9C2910AC6C96C3315B40F754...
SHA-512	B7944AFB7948DEEEA45511A5A3749...
SHA3-256	2F163014C88134F44C36F7C081B7D...
SHA3-512	3830C56E8AD2A703FF8514D3F6C9D...

I opened the files properties and then investigated its file hashes where I found the md5 hash

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

Answer the questions below

The MD5 Checksum of aws.exe

D2778164EF643BA8F44CC202 ✓ Correct Answer

The MD5 Checksum of NetLogo.exe

59CB421172A89E1E16C11A42 ✓ Correct Answer

The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF ✓ Correct Answer

Task 8 Now lets see if the MD5 Checksums have been analysed before

File Explorer showing vlc Properties. File Hashes tab selected. MD5 hash: 700197A0D7120876797A5A411797...

Woop woop! Your answer is correct

1.5 Now lets see if the MD5 Checksums have been analysed before

Questions

Answer the questions below

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

Nay ✓ Correct Answer

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

Nay ✓ Correct Answer

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

Nay ✓ Correct Answer

Task 9 Identifying if the Executables are obfuscated / packed

Task 10 What is Obfuscation / Packing?

File Explorer showing NetLogo Properties. File Hashes tab selected. MD5 hash: F06C526E5C888B594F69FC618BE...

Woop woop! Your answer is correct

I checked the md5 hashes against the virustotal tool for reports on them being malicious, below are results as follows, aws.exe, netlogo.exe, vlc.exe

Community Score 104 / 72

File distributed by Microsoft, Android Studio and others.

28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a

system_embedded_python_Lib_site-packages_Setuptools_cli-64.exe

Size 73.00 KB | Last Analysis Date 2 days ago | EXE

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 25+

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

Security vendor	Result	Do you want to automate checks?
Acronis (Static ML)	Undetected	AhnLab-V3 Undetected
Alibaba	Undetected	AliCloud Undetected
ALYac	Undetected	Antiy-AVL Undetected

Community Score 1 / 72

1/72 security vendor flagged this file as malicious

e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536

NetLogo.exe

Size 49.00 KB | Last Analysis Date 1 day ago | EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Security vendor	Result	Do you want to automate checks?
Jiangmin	Backdoor.Lotok.cfq	Acronis (Static ML) Undetected
AhnLab-V3	Undetected	Alibaba Undetected
AliCloud	Undetected	ALYac Undetected

1.6 Identifying if the Executables are obfuscated / packed

Questions

I launched the PEid tool located in the Documents folder, to find the packer of two files located in the task 9 folder, and this was the results

Room progress (66%)

File Offset: 0000424D First Bytes: 55,88,EC,53
Linker Info: 6.0 Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL [Overlay]

Multi Scan Task Viewer Options About Exit
Stay on top

An example of using PEiD to identify the packer of a file. In this case, it is reported as "Microsoft Visual C++ 6.0"

Answer the questions below

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

Microsoft Visual C++ 6.0 DLL ✓ Correct Answer Hint

What does PeID propose AD29AA1B.bin being packed with?

Microsoft Visual C++ 6.0 ✓ Correct Answer

Task 10 What is Obfuscation / Packing?

1.7 What is Obfuscation / Packing?

Questions

Used the PEid tool to check the file in task 10 what its packed with this was the results.

Room progress (70%)

like us reversing it to understand its behaviours and ultimately with the aims of achieving infection.

How packing works is out of scope for this room, but I hope to be able to delve into topics like these later on within THM, so that you can understand the theory behind the practical skills you'll be using.

Practical:

Your task is to identify whether or not the file "6F431F46547DB2628" located in the Directory of "Tasks\Task 10" is packed using the tool "PeID" akin to the task you just completed!

Answer the questions below

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

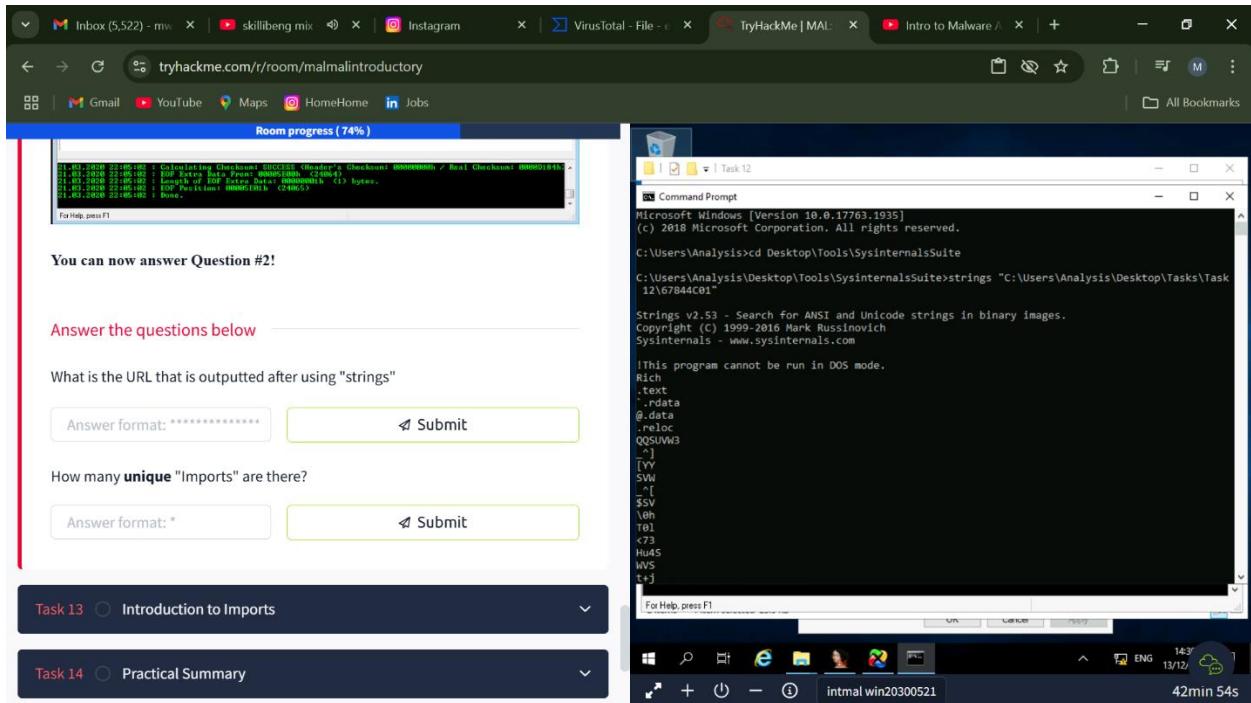
FSG 1.0 -> dulek/xt ✓ Correct Answer

Task 11 Visualising the Differences Between Packed & Non-Packed Code

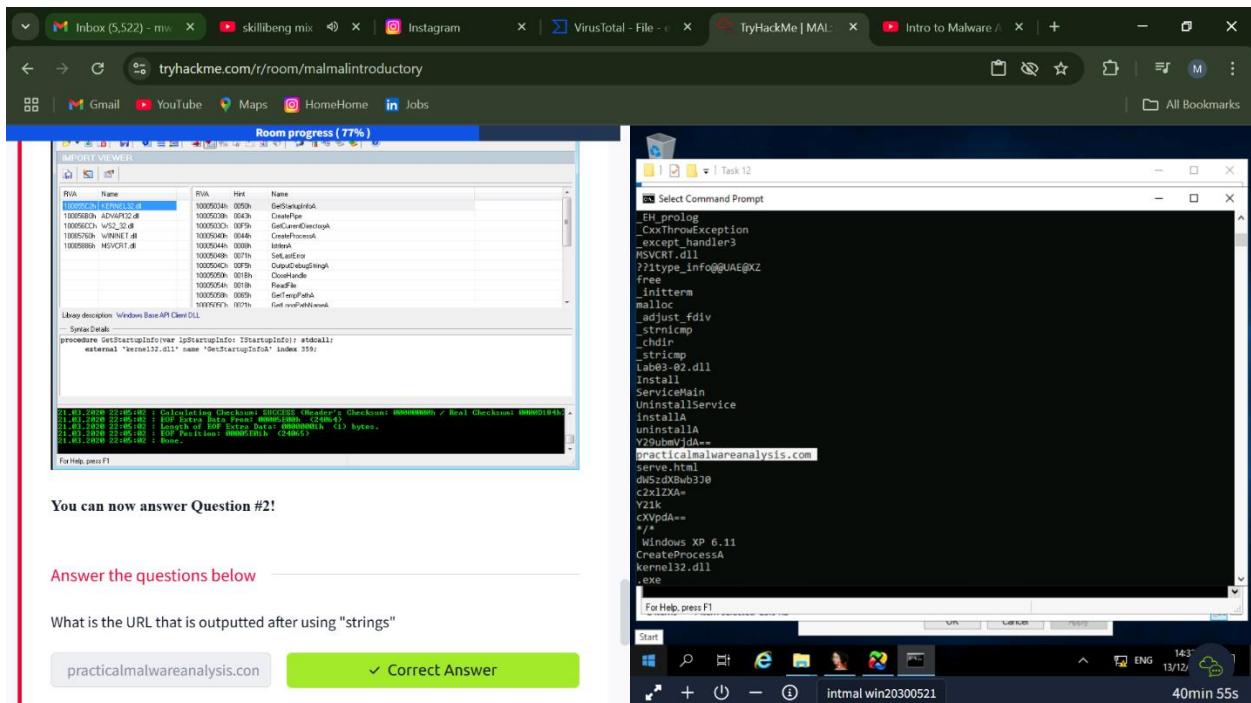
1.8 Introduction to Strings

Questions

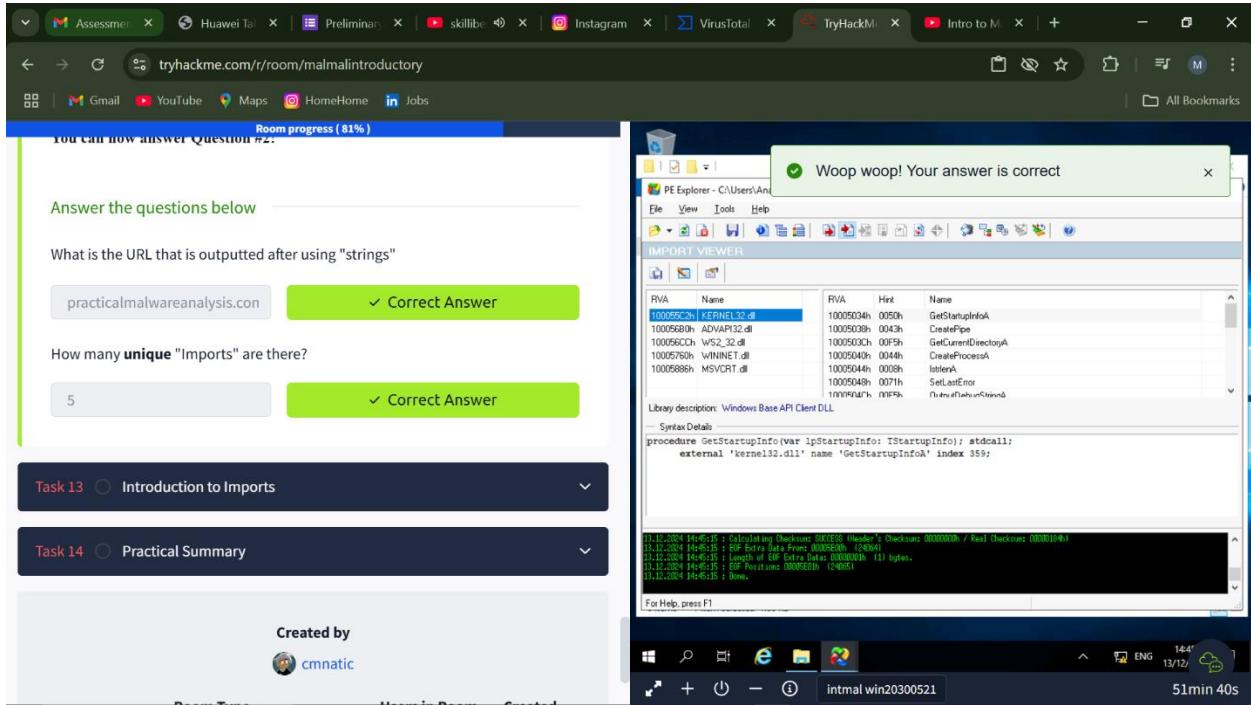
I started off by opening the cmd and navigating to the sysinternalsSuite folder and used string program to output the strings in the file in task 12 folder.



After running the command I found quite a number of strings outputted and among them was a URL.



I opened the file in task 12 folder with PE explorer where I viewed the imports and found there were 5 imports done.



1.9 Introduction to Imports

Questions

With use of IDA tool I opened install.exe file in task 13 folder, after opening I investigated the imports of msi and found to be 9.

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

Task 14 Practical Summary

Created by cmnatic

Room Type	Users in Room	Created
Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	67,232	1728 days ago

1.10 Practical Summary

Questions

I investigated the properties of the complexcalculator file by looking at its hashes where I found the md5 hash

I'm not going to walk you through this one, but you have done all the necessary steps above to achieve this. GL HF :^)

If you struggle, revisit the techniques you used above. Moreover, if you're still stuck, visit the [TryHackMe Discord!](#)

The file specified for analysis is "**ComplexCalculator.exe**" in the **Directory** "**Tasks/Task 14**". I'll leave it up to you to figure out what tool(s) out of what we've used above is best!

Answer the questions below

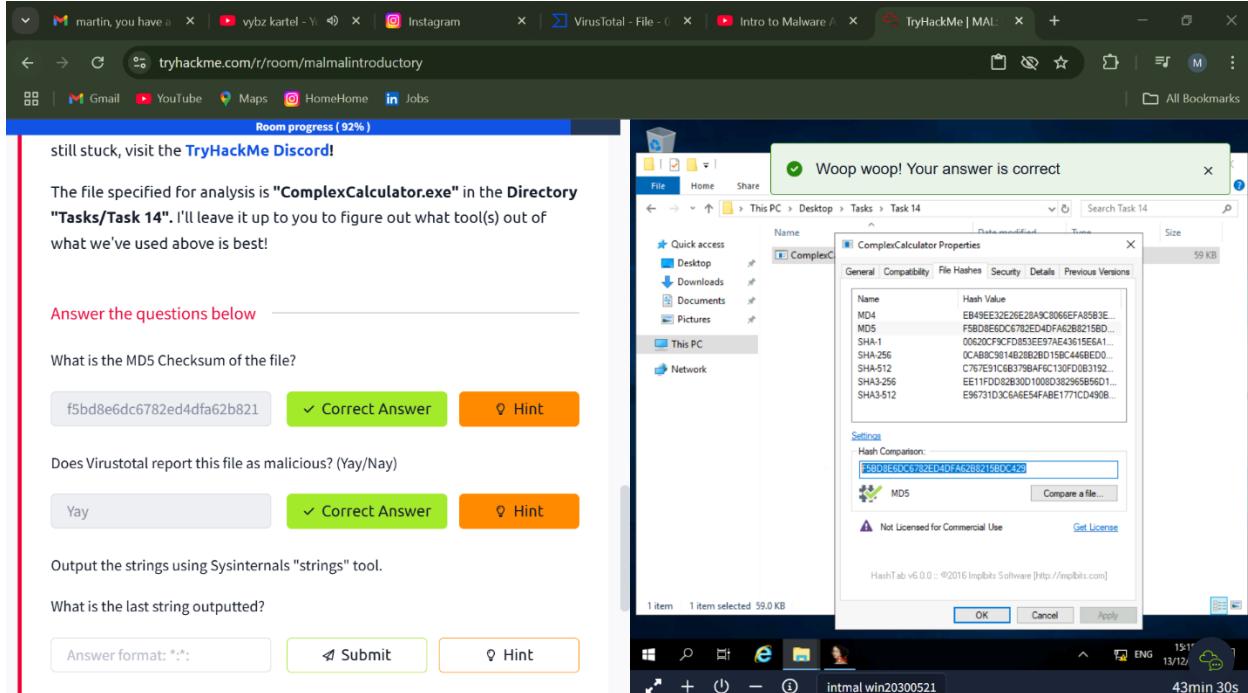
What is the MD5 Checksum of the file?

f5bd8e6dc6782ed4dfa62b821 ✓ Correct Answer ⚡ Hint

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

Answer format: *** ↗ Submit ⚡ Hint

Looking at the md5 hash I found against the virustotal tool I found it to be reported to be malicious, the results are below.



The file specified for analysis is "ComplexCalculator.exe" in the Directory "Tasks/Task 14". I'll leave it up to you to figure out what tool(s) out of what we've used above is best!

Answer the questions below

What is the MD5 Checksum of the file?

f5bd8e6dc6782ed4dfa62b821 ✓ Correct Answer ⚡ Hint

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

Yay ✓ Correct Answer ⚡ Hint

Output the strings using Sysinternals "strings" tool.

What is the last string outputted?

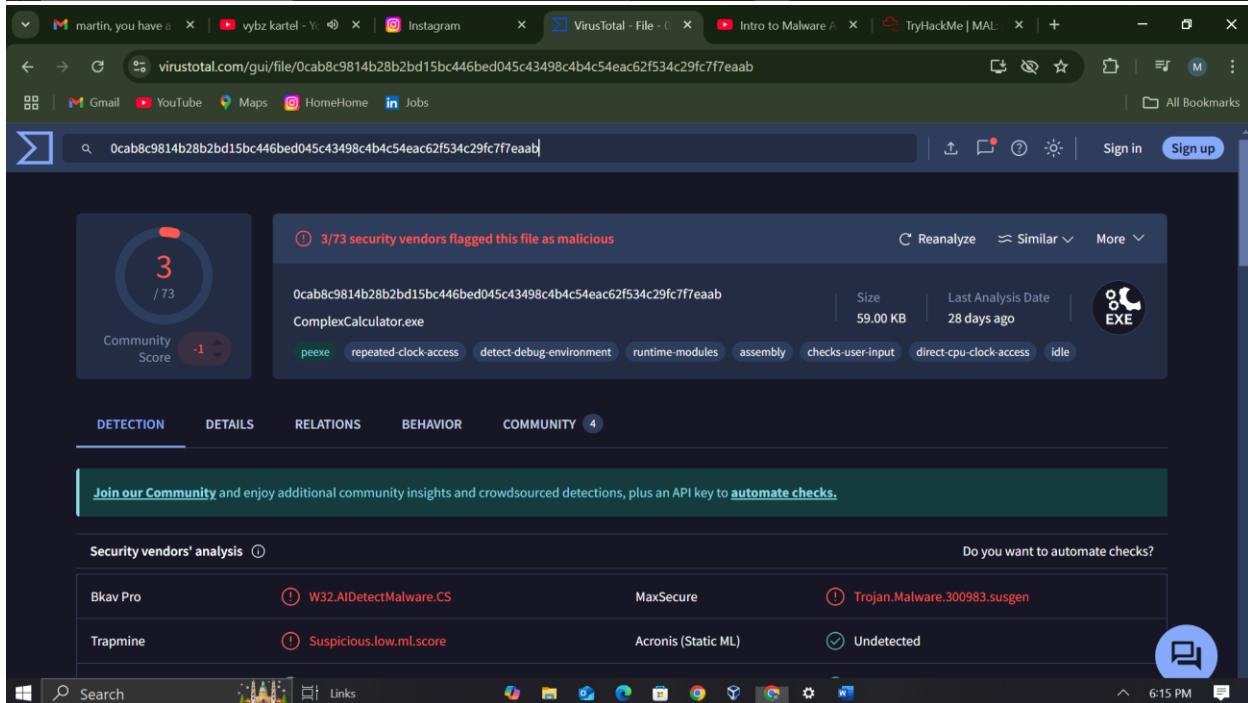
Answer format: *.*: ✓ Submit ⚡ Hint

Woop woop! Your answer is correct

File Explorer showing ComplexCalculator Properties

Name	Hash Value
MD4	EB49EE32E26E28A9C8066EFA85B3E...
MD5	F5B08E5DC0D6782ED4DFAE2B8215BD...
SHA-1	00620C9FCF053E97AE43615E5A1...
SHA-256	0CA8C9814B20B2BD15BC446BED045...
SHA-512	C767E91C6B378AFCFC130FD03192...
SHA3-256	EE11FDD0283010080382965B565D1...
SHA3-512	E96731D3C6A6E54FABE1771CD490B...

HashTab v6.0.0 - ©2016 Impbits Software [http://mpbitz.com]



3/73 security vendors flagged this file as malicious

0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab

ComplexCalculator.exe

Community Score: 3 / 73

Size: 59.00 KB | Last Analysis Date: 28 days ago

PE executable (EXE)

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

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

Security vendors' analysis

Bkav Pro	W32.AIDetectMalware.CS	MaxSecure	Trojan.Malware.300983.susgen
Trapmine	Suspicious.low.ml.score	Acronis (Static ML)	Undetected

Do you want to automate checks?

I started off by opening the cmd and navigating to sysinternalssuite folder to use the string program so as to find output of strings in the complexcalculator file. Plus found the last string as the answer.

The screenshot shows a web browser with multiple tabs open. The main content area displays a 'Practical Summary' for 'Task 14'. It includes a note about completing previous steps, a message from the author, and a section for answering questions. Below this, there are two questions with answer input fields and buttons for 'Correct Answer' and 'Hint'. To the right of the browser, a Windows Command Prompt window is running the command 'strings "C:\Users\Analysis\Desktop\Tasks\Task 14\ComplexCalculator.exe"'. The output of the command is displayed in the window, showing various strings extracted from the executable. The task progress bar at the top indicates 92% completion.

Room progress (92%)

Task 14 Practical Summary

I'm not going to walk you through this one, but you have done all the necessary steps above to achieve this. GL HF :^)

If you struggle, revisit the techniques you used above. Moreover, if you're still stuck, visit the [TryHackMe Discord!](#)

The file specified for analysis is "**ComplexCalculator.exe**" in the Directory "**Tasks/Task 14**". I'll leave it up to you to figure out what tool(s) out of what we've used above is best!

Answer the questions below

What is the MD5 Checksum of the file?

f5bd8e6dc6782ed4dfa62b821

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

Yay

Manage Task 14

Command Prompt

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

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
SysInternals - www.sysinternals.com

!This program cannot be run in DOS mode.

a'A
od.
Vc.
od*
od
od+
1g*
1g-
Rich%
.TEXT
`.rdata
@.data
.rsrc
@.reloc
pp08
pp09
%{T
po9
%{T
%{U
|[<
```

1 item 1 item selected 59.0 KB

Task View

152° 13/12

38min 0s

martin, you have a | vybz kartel - Y | Instagram | VirusTotal - File - 0 | Intro to Malware A | TryHackMe | MAL: | + | - | X

All Bookmarks

Room progress (96%)

If you struggle, revisit the techniques you used above. Moreover, if you're still stuck, visit the [TryHackMe Discord!](#)

The file specified for analysis is "**ComplexCalculator.exe**" in the Directory "**Tasks/Task 14**". I'll leave it up to you to figure out what tool(s) out of what we've used above is best!

Answer the questions below

What is the MD5 Checksum of the file?

f5bd8e6dc6782ed4dfa62b821

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

Yay

Output the strings using Sysinternals "strings" tool.

What is the last string outputted?

d:h:

Manage Task 14

Select Command Prompt

```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<trustInfo xmlns="urn:schemas-microsoft-com:com:asm.v3">
<requestedPrivileges>
<requestedExecutionLevel level='asInvoker' uiAccess='False' />
</requestedPrivileges>
</trustInfo>
</assembly>
:z:-+17+-:C:I:O:U[:a:g:m:s:y:
-)
1 181,12181>iD1J1P1
12282>2
283,3B3U3
585,5m5
60d
7-7,7V7A7
88BV8J8
':;h:n;
::@#e;m;w;
</><:D@I<0<Y<<<
=6=A=F=L+V="S=x=
>@>P>_>
?@?H?Q?^?v?
0@111p1t1
2_2
d:h:
```

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

1 item 1 item selected 59.0 KB

Type here to search

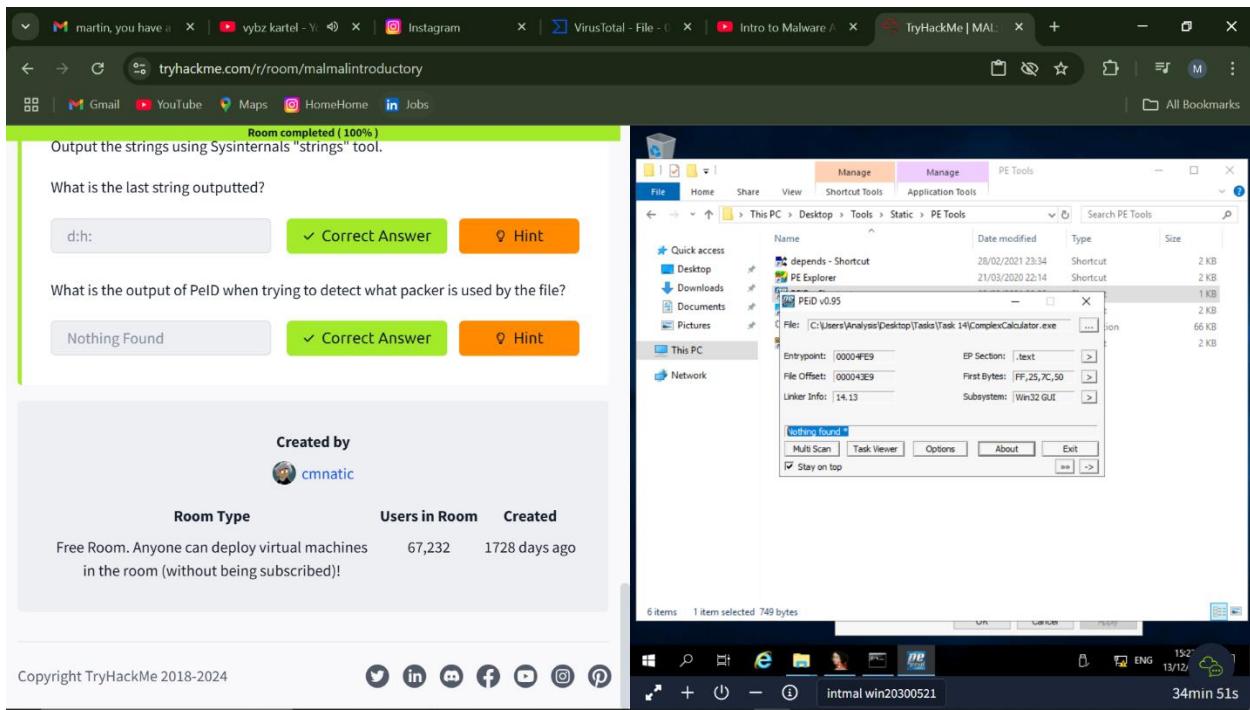
152° 13/12

37min 29s

martin, you have a | vybz kartel - Y | Instagram | VirusTotal - File - 0 | Intro to Malware A | TryHackMe | MAL: | + | - | X

All Bookmarks

Used PEiD to find the packer of the complexcalculator file and found it to be nothing.



2.0 Conclusion

This room has been helpful on how to conduct malware analysis and also to review or assess an application or file that looks suspicious, by looking at its MD5 hash and checking it against the virustotal tool.