

Report on Malware Introductory

Task 1: What is the Purpose of Malware Analysis?

Malware analysis is crucial for understanding the behavior, functionality, and impact of malicious software (malware). Its primary purposes include:

- **Detection and Classification:** Identifying the type of malware (e.g., virus, worm, trojan) to develop appropriate defenses.
- **Behavioral Analysis:** Understanding what actions the malware performs on infected systems.
- **Reverse Engineering:** Deconstructing malware to uncover its algorithms, protocols, and communication methods.
- **Attribution:** Determining the origin or authorship of the malware.
- **Defensive Measures:** Developing countermeasures and mitigations against current and future malware threats.

Task 2: Understanding Malware Campaigns

Malware campaigns refer to coordinated efforts by threat actors to distribute and execute malicious software across multiple targets. Key aspects include:

- **Attack Vectors:** How malware spreads (e.g., phishing emails, exploit kits, malicious websites).
- **Targets:** Types of systems or networks vulnerable to the malware.
- **Goals:** Objectives of the malware campaign (e.g., data theft, system disruption, espionage).
- **Lifecycle:** Phases from initial infection to execution and persistence.
- **Attribution:** Linking campaigns to specific threat actors or groups.

Task 3: Identifying if a Malware Attack has Happened

Signs of a malware attack include:

- Unexplained system slowdowns or crashes.
- Unexpected network activity or outgoing connections.
- Changes in system settings or files.
- Anti-virus alerts or warnings.
- Unauthorized access or data breaches.

Task 4: Static Vs. Dynamic Analysis

- **Static Analysis:** Examines the malware without executing it. Involves examining code, file structure, and metadata.
- **Dynamic Analysis:** Involves executing the malware in a controlled environment (sandbox) to observe behavior, interactions, and network activity.

Task 5: Discussion of Provided Tools & Their Uses

Common tools for malware analysis include:

- **Static Analysis Tools:** IDA Pro, Ghidra, PE Explorer.
- **Dynamic Analysis Tools:** Cuckoo Sandbox, Hybrid Analysis.
- **Utilities:** Wireshark for network traffic analysis, Process Monitor for system activity monitoring.

Task 6: Connecting to the Windows Analysis Environment (Deploy)

Setting up a Windows analysis environment involves:

- Using virtualization software like VMware or VirtualBox.
- Installing a clean, isolated instance of Windows for testing malware safely.

Task 7: Obtaining MD5 Checksums of Provided Files

MD5 checksums are obtained to verify file integrity and detect changes or tampering.

Task 8: Checking if MD5 Checksums have been analyzed before

Comparison of MD5 checksums against databases or online repositories (e.g., VirusTotal) to determine if the file has been previously analyzed or identified as malware.

Task 9: Identifying if the Executables are obfuscated / packed

Detection of obfuscation or packing techniques used to conceal the true purpose of executables.

Task 10: What is Obfuscation / Packing?

- **Obfuscation:** Techniques to make code difficult to understand or analyze.

- **Packing:** Compression and encryption methods used to reduce file size and hinder analysis.

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

Packed code appears as compressed or encrypted blocks, while non-packed code is more readable and structured.

Task 12: Introduction to Strings

Strings are sequences of characters within executable files that can reveal important information about functionality, behavior, or embedded resources.

Task 13: Introduction to Imports

Imports refer to external functions or libraries called by executable files, providing insights into dependencies and functionality.

Task 14: Practical Summary

Malware analysis is essential for cybersecurity to understand, detect, and mitigate the impact of malicious software. It involves static and dynamic analysis techniques, the use of specialized tools, and understanding malware behaviors and campaign strategies. By deploying analysis environments and utilizing tools effectively, security professionals can better defend against evolving threats.

Screenshot Overview of the Task

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/malmainintroductory

Dashboard Learn Compete Other

Access Machines Go Premium 6

WHAT IS THE PURPOSE OF MALWARE ANALYSIS?

Malware is such a prevalent topic within Cybersecurity, and often an unfortunately recurring theme among global news today.

Not only is malware analysis a form of incidence response, but it is also useful in understanding how the behaviours of variants of malware result in their respective categorisation. This room will be a practical introduction to the techniques and tools used throughout malware analysis - albeit brief, I hope to expand on these techniques a lot more in-depth within the future.

When analysing malware, it is important to consider the following:

- Point of Entry (PoE) i.e. Was it through spam that our e-mail filtering missed and the user opened the attachment? Let's review our spam filters and train our users better for future prevention!
- What are the indicators that malware has even been executed on a machine? Are there any files, processes, or perhaps any attempt of "un-ordinary" communication?
- How does the malware perform? Does it attempt to infect other devices? Does it encrypt files or install anything like a backdoor / Remote Access Tool (RAT)?
- Most importantly - can we ultimately prevent and/or detect further infection?!

Answer the questions below

Ah, now I kinda understand...

No answer needed ✓ Correct Answer

Task 2 Understanding Malware Campaigns

18°C Mostly cloudy

Search

9:08 PM 7/25/2024

cs-sa07-24019

John_Mbithi_Mutave

Kaspersky report on the "Crouching Yeti (Energetic Bear)" campaign, this campaign specifically targets the following:

- Industrial/machinery
- Manufacturing
- Pharmaceutical
- 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

Recall overview, this classification of signatures are the observation of any networking communication taking place during delivery, execution and propagation. For example, in Ransomware, where has the Malware contacted for Bitcoin payments?

Such as in the case of Wannacry, looking for a large amount of "Samba" Protocol communication attempts is a great indication of infection due to its use of "Eternalblue".

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

Task 4 ✓ Static Vs. Dynamic Analysis

Whilst the methods and tools used for these two categories are vastly different, they are essential in composing an understanding of how a malware behaves.

Static Analysis.

At its brief, "Static Analysis" is used to gain a high-level abstraction of the sample - it can be fairly simple to decide if a piece of code is "malicious" or not with this method alone (but not always, this will be discussed later...). At its core, this method is of the analysis of the sample at the state it presents itself as, without executing the code.

Employing the use of techniques such as signature analysis via checksums means quick, efficient (albeit extremely brief) and safe analysis of malware.

Dynamic Analysis

This step is a lot more involved, and is where the abstraction of the sample is largely built upon. "Dynamic Analysis" essentially involves executing the sample and observing what happens. This of course is not safe. If the sample turns out to be "Ransomware" - you've now lost your files. If it is capable of propagating via traversing a network, nice...You've now just infected your Local Area Network (LAN).

Please note that these are extremely simplistic explanations of these techniques, there is a lot more involved which we will go throughout this series.

Answer the questions below

I understand the two broad categories employed when analysing potential malware!

No answer needed ✓ Correct Answer

Task 5 Discussion of Provided Tools & Their Uses

PEID
PE Explorer
PExview
ResourceHacker

C:\Users\Analysis\Desktop\Tools\Static\Disassembly

- IDA Freeware
- WinDbg

C:\Users\Analysis\Desktop\Tools\Sysinternalsuite

- ResourceHacker

C:\Users\Analysis\Desktop\Tools\Dynamic

The tools listed here will be used for future tasks, as they involve debugging which is currently out-of-scope for this room...However, will be explored later within the series.

Answer the questions below

Lets proceed

No answer needed ✓ Correct Answer

Task 6 Connecting to the Windows Analysis Environment (Deploy)

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web browser window with multiple tabs open. The active tab is for the TryHackMe challenge room 'malmailintroductory'. The page displays instructions for connecting via RDP using Remmina, with the IP address set to 192.168.0.48 and the username ANALYST-PC\Analysis. Below this, there's a note about replacing the IP with **MACHINE_IP**. A screenshot of the Remmina client interface is shown, with 'RDP' selected and the IP 192.168.0.48 entered. The task bar at the bottom indicates 'Task 7' and 'Obtaining MD5 Checksums of Provided Files'. The Windows desktop environment visible includes a weather widget (18°C, Mostly cloudy), a taskbar with various icons (Search, File Explorer, Google Chrome, etc.), and system status indicators (Wi-Fi, battery, time: 9:10 PM, date: 7/25/2024).

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a Windows desktop environment with multiple windows open:

- Browser Window:** tryhackme.com//room/malintroductory. The page displays "MAL: Malware Introductory" with a lock icon, indicating an introductory room for malware analysis. It shows a progress bar at 37%.
- HxD Hex Editor:** A window titled "HxD - [C:\Users\Analysis\Desktop\Tasks\Task 7\aws.exe]" is open, showing the binary file "aws.exe". The "Data inspector" tab is selected, displaying memory offsets from 00 to 00000070. The byte value at offset 00000070 is highlighted as 77 (Int8). The status bar indicates "47min 42s".
- File Explorer:** Shows a folder structure under "Tasks" containing "aws.exe".
- Recycle Bin:** Shows a single item: "aws.exe".
- Task View:** Shows a list of running applications including "Inbox", "CSA2-2024", "TryHackMe", "AWS - Next", "AWS Program", and "AWS Feed".
- System Tray:** Shows the date and time as "24/07/2024 8:14 PM", battery level, and network status.

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a Windows desktop environment with a browser window open to the TryHackMe website. The browser has multiple tabs and several windows are visible on the desktop.

Browser Window Content:

- The MD5 Checksum of aws.exe is D2778164EF643BA8F44CC202EC7EF157. This is a correct answer.
- The MD5 Checksum of NetLogo.exe is 59CB421172A89E1E16C11A428326952C. This is a correct answer.
- The MD5 Checksum of vlc.exe is listed as "Answer format: *****". A "Submit" button is present.
- A dropdown menu for Task 8 says "Now lets see if the MD5 Checksums have been analysed before".
- A dropdown menu for Task 9 says "Identifying if the Executables are obfuscated / packed".
- A dropdown menu for Task 10 says "What is Obfuscation / Packing?".
- A dropdown menu for Task 11 says "Visualising the Differences Between Packed & Non-Packed Code".
- A dropdown menu for Task 12 says "Introduction to Strings".

Desktop Environment:

- File Explorer window showing tasks and tools.
- Notepad++ window.
- HxD Hex Editor window showing the contents of NetLogo.exe. The offset (h) 00 01 02 03 row shows values 00 00 00 00, 00 00 00 00, 00 00 00 00, and 00 00 00 00 respectively.
- Taskbar showing various open applications including a browser, file explorer, and system tray.
- System tray showing battery level (18:36), language (ENG), date (24/07/2024), and time (8:35 PM).

Second Browser Window Content:

- The MD5 Checksum of aws.exe is D2778164EF643BA8F44CC202EC7EF157. This is a correct answer.
- The MD5 Checksum of NetLogo.exe is 59CB421172A89E1E16C11A428326952C. This is a correct answer.
- The MD5 Checksum of vlc.exe is S416BE1B8B04B1681CB39CF0E2CAAD9F. This is a correct answer.
- A dropdown menu for Task 8 says "Now lets see if the MD5 Checksums have been analysed before".
- A dropdown menu for Task 9 says "Identifying if the Executables are obfuscated / packed".
- A dropdown menu for Task 10 says "What is Obfuscation / Packing?".
- A dropdown menu for Task 11 says "Visualising the Differences Between Packed & Non-Packed Code".
- A dropdown menu for Task 12 says "Introduction to Strings".

Desktop Environment (Second View):

- File Explorer window showing tasks and tools.
- Notepad++ window.
- HxD Hex Editor window showing the contents of vlc.exe. The offset (h) 00 01 02 03 row shows values 00 00 00 00, 00 00 00 00, 00 00 00 00, and 00 00 00 00 respectively.
- Taskbar showing various open applications including a browser, file explorer, and system tray.
- System tray showing battery level (18:39), language (ENG), date (24/07/2024), and time (8:39 PM).

cs-sa07-24019

John_Mbithi_Mutave

Your Task:
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
D2778164EF643BA8F44CC20EC7EF157 ✓ Correct Answer

The MD5 Checksum of Netlogo.exe
59CB421172A89E1E16C11A428326952C ✓ Correct Answer

The MD5 Checksum of vlc.exe
5416BE1B8B04B1681CB39CF0E2CAAD9F ✓ Correct Answer

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

Task 7 Obtaining MD5 Checksums of Provided Files

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

Outside of the Remote Windows Environment i.e. Kali or your Windows PC, look up those MD5 "Checksums" on Virustotal to solve this task:

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

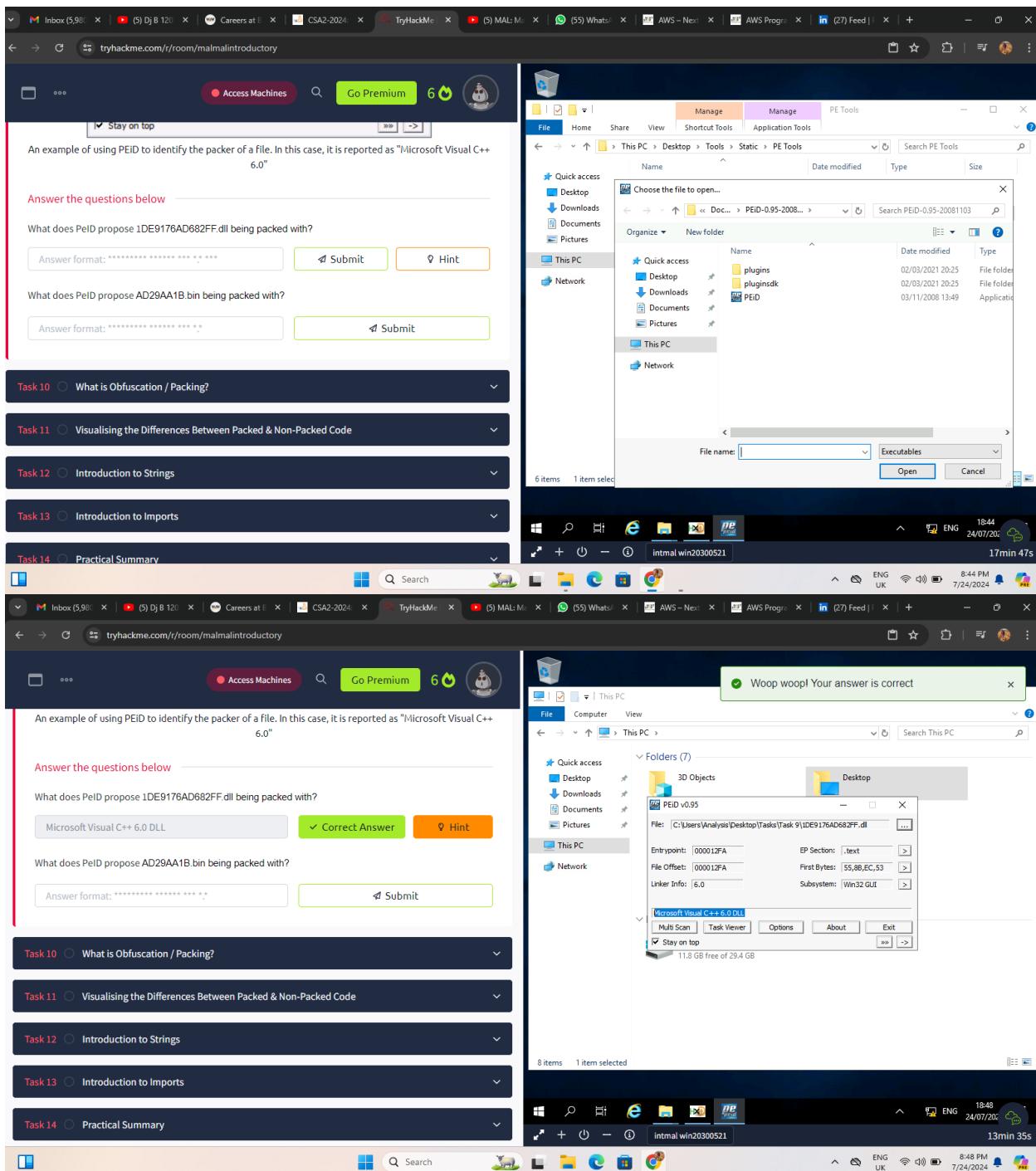
Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)
Nay ✓ Correct Answer

Task 9 Identifying if the Executables are obfuscated / packed

Windows Taskbar and System tray showing the analysis process.

cs-sa07-24019

John_Mbithi_Mutave



cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a Windows desktop environment with a browser window open to the TryHackMe website. The browser has multiple tabs, including 'Inbox (5,96)', '(5) Dj B 120', 'Careers at...', 'CSA2-2024...', 'TryHackMe', '(5) MAL: Mi...', '(55) What...', 'AWS - Next...', 'AWS Progra...', and '(27) Feed'. The main content of the browser window is a challenge titled 'Task 9' from the 'malmainintroductory' room. It asks about file packing and provides two dropdown answers: 'Microsoft Visual C++ 6.0 DLL' and 'Microsoft Visual C++ 6.0'. A green button labeled 'Correct Answer' is visible. Below the dropdowns, there are questions about what PeID proposes for specific files: '1DE9176AD682FF.dll' and 'AD29AA1B.bin'. The desktop background is a light blue gradient.

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?

Answer format: ***** * * * * * Submit

Task 10: What is Obfuscation / Packing?

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

Task 12: Introduction to Strings

Task 13: Introduction to Imports

Task 14: Practical Summary

File Explorer window (This PC):

- Desktop
- Downloads
- Documents
- Pictures
- This PC
- Network

Choose the file to open... (Task 9)

Name	Date modified	Type
1DE9176AD682FF.dll	19/12/2010 17:16	Application
AD29AA1B.bin	08/01/2012 08:19	BIN File

File name: DE9176AD682FF

Open Cancel

Taskbar:

- Inbox (5,96)
- (5) Dj B 120
- Careers at...
- CSA2-2024...
- TryHackMe
- (5) MAL: Mi...
- (55) What...
- AWS - Next...
- AWS Progra...
- (27) Feed
- intmal.win20300521

18:49 24/07/2024 12min 53s

File Explorer window (This PC):

- 3D Objects
- Desktop

PEID v0.95

File:	EntryPoint:	EP Section:	First Bytes:	Linker Info:	Subsystem:
C:\Users\Analysis\Desktop\Tasks\Task 9\1DE9176AD682FF.dll	000012FA	.text	55,8B,EC,53	6.0	Win32 GUI

Microsoft Visual C++ 6.0 DLL

Multi Scan Task Viewer Options About Exit

Stay on top

12.2 GB free of 23.4 GB

File Explorer status bar: 8 items 1 item selected

Taskbar:

- Inbox (5,96)
- (5) Dj B 120
- Careers at...
- CSA2-2024...
- TryHackMe
- (5) MAL: Mi...
- (55) What...
- AWS - Next...
- AWS Progra...
- (27) Feed
- intmal.win20300521

18:49 24/07/2024 12min 25s

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a Windows desktop environment with a browser window open to tryhackme.com/r/room/malmailintroductory. The browser displays a task titled "Task 12" which involves using PEID to identify a file's packer. The PEID tool interface is overlaid on the browser window, showing details for a file named "Task 12\6784C01". The "Microsoft Visual C++ 6.0 DLL [Overlay]" tab is selected. The task asks: "What does PeID propose 1DE9176AD682FF.dll being packed with?". Below the task, there are two input fields: "Microsoft Visual C++ 6.0 DLL" and "Microsoft Visual C++ 6.0". The first field has a "Correct Answer" button next to it, which is highlighted in green. The second field has a "Hint" button next to it. The task also includes a "Stay on top" checkbox. The background of the desktop shows a File Explorer window titled "This PC" with several items listed, including a PEID v0.95 executable and a Microsoft Visual C++ 6.0 DLL file. The system tray at the bottom right shows the date and time as 24/07/2024, 8:50 PM, and battery level as 12min 7s.

File: C:\Users\Analysis\Desktop\Tasks\Task 12\6784C01

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]

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?

File Computer View This PC Desktop Downloads Documents Pictures Network

PEID v0.95

File: C:\Users\Analysis\Desktop\Tasks\Task 9\1DE9176AD682FF.dll

Entrypoint: 000012FA EP Section: .text

File Offset: 000012FA First Bytes: 55,8B,EC,53

Linker Info: 6.0 Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL

Multi Scan Task Viewer Options About Exit

Stay on top

12.2 GB free of 29.4 GB

8 items 1 item selected

Windows taskbar: intmal win20300521

System tray: ENG 24/07/2024 8:50 PM 7/24/2024 12min 7s

tryhackme.com/r/room/malmailintroductory

Access Machines Go Premium 6

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

Task 12 ○ Introduction to Strings

Task 13 ○ Introduction to Imports

Task 14 ○ Practical Summary

Created by cmnatic Room Type Free Room. Anyone can deploy virtual machines Users in Room 61,591 Created 1586 days ago

File Computer View This PC Desktop Downloads Documents Pictures Network

PEID v0.95

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

Multi Scan Task Viewer Options About Exit

Stay on top

HxD - [C:\Users\Analysis\Desktop\Tasks\Task 7\vc.exe]

File Computer View This PC Desktop Downloads Documents Pictures Network

Windows taskbar: intmal win20300521

System tray: ENG 24/07/2024 8:51 PM 7/24/2024 10min 21s

Screenshot of a browser window showing a list of obfuscated API calls from PEID v0.95 analysis. The list includes functions like `IbvC_SetUserAgent`, `IbvC_...`, `CryptAcquireContextA`, `CryptGenRandom`, `CryptReleaseContext`, `RegOpenKeyExW`, `RegQueryValueExW`, `CloseHandle`, `CreateFileW`, `CreateSemaphoreW`, `CreateThread`, `DeleteCriticalSection`, `DeleteFileW`, `DuplicateHandle`, `EnterCriticalSection`, `FindFileW`, `FindFirstFileW`, `FreeLibrary`, and `GetCommandLineW`. Below the list, a note says: "See how there's so much more information here? Obfuscated code is much harder to analyze at least at the static level, as we're presented with very little information!"

Answer the questions below

Cursed obfuscation!

No answer needed ✓ Correct Answer

Task 12 Introduction to Strings

Screenshot of a browser window showing a task titled "Introduction to Strings". The task description says: "Open a Command prompt on the Windows Machine and navigate to the directory "Tools\SysinternalsSuite". Keep this terminal open. We're going to use Microsoft's Sysinternals "Strings" program to output the retained strings within the specified file in "Task 12". We can do this by: strings "C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01" You will receive a whole load of text, most of it looks like nonsense...But there is some text in there that is valuable. Scroll up!"

Task:

Open a Command prompt on the Windows Machine and navigate to the directory "Tools\SysinternalsSuite".

```
cd C:\Users\Analysis\Desktop\Tools\SysinternalsSuite
```

Keep this terminal open.

We're going to use Microsoft's Sysinternals "Strings" program to output the retained strings within the specified file in "Task 12". We can do this by:

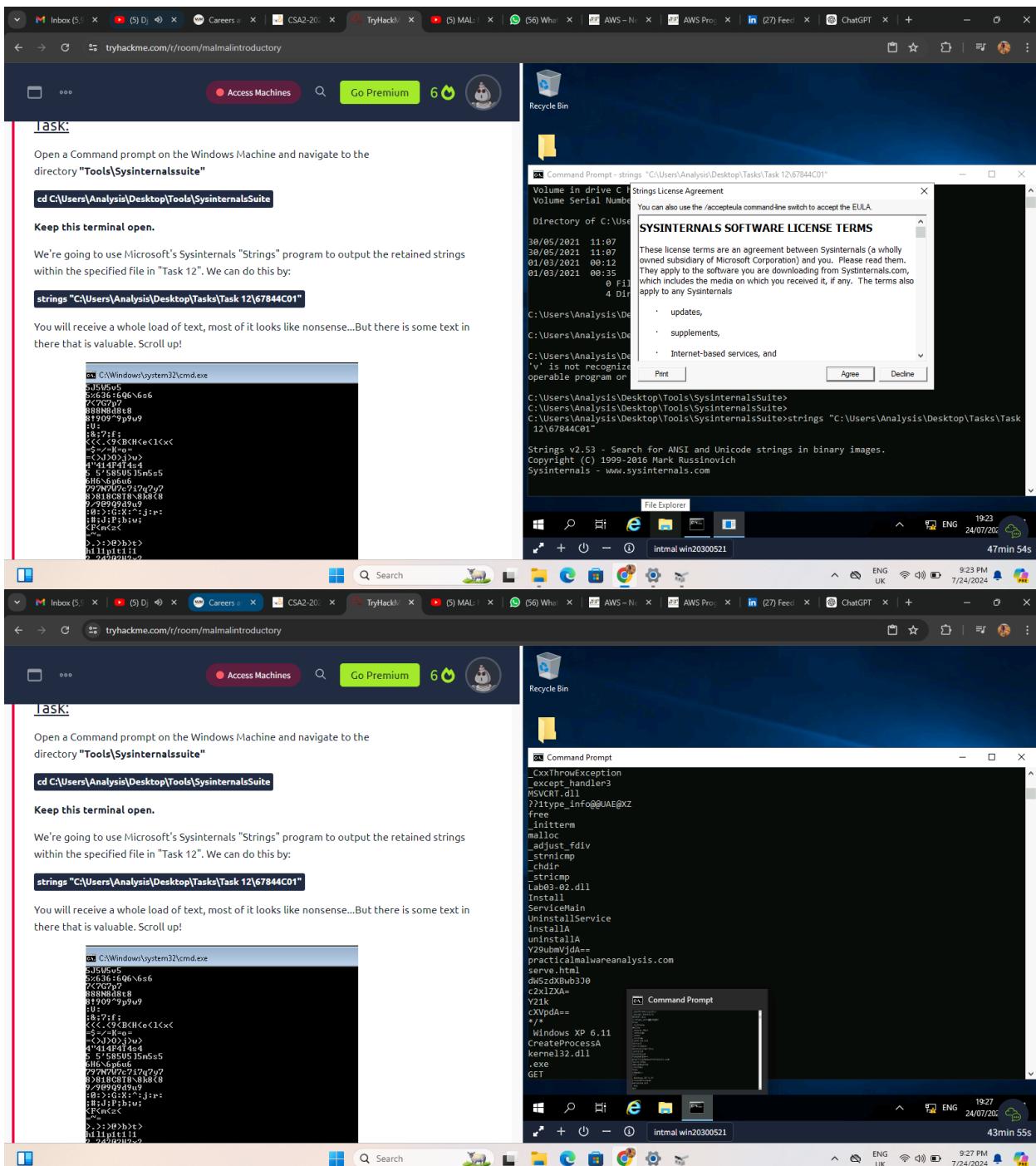
```
strings "C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01"
```

You will receive a whole load of text, most of it looks like nonsense...But there is some text in there that is valuable. Scroll up!

Screenshot of a terminal window showing the output of the `strings` command. The output is a long list of binary strings, including some recognizable text like "C:\Windows\system32\cmd.exe", "E:\636-1606\6e6", and "81909^9f99".

cs-sa07-24019

John Mbithi Mutave



cs-sa07-24019

John_Mbithi_Mutave

You can now answer Question #2!

Answer the questions below

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

practicalmalwareanalysis.com ✓ Correct Answer

How many unique "Imports" are there?

Answer format: * Submit

Task 13 Introduction to Imports

Task 14 Practical Summary

Created by cmmatic Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed!) Users in Room 61,591 Created 1586 days ago

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

File View Tools Help

To start exploring executable files, click File | Open File [Ctrl+O] Alternatively, you can drag and drop a file into PE Explorer

What PE Explorer Does

PE File Viewer Export/Import Viewer Section Viewer/Editor Digital Signature Viewer Resource Viewer/Editor Win32 Disassembler Dependency Scanner String Tools

How to buy Continue Quit

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

For Help, press F1

Address of Entry Point: 10004E00 Real Image Checksum: 00000104h

Field Name	Data Value	Description
Machine	014Ch	386®
NumberOfSections	00000008h	
TimeDateStamp	4C413E29h	28/09/2010 01:00:25
PointerToSymbolTable	00000000h	
NumberOfSymbols	00000000h	
SizeOfOptionalHeader	00E0h	
Characteristics	210Eh	PE32
Magic	010Bh	6.0
LinkerVersion	0006h	
SizeOfCode	00004000h	
SizeOfInitializedData	0000CA00h	
SizeOfUninitializedData	00000000h	
AddressOfEntryPoint	10004E00h	
BaseOfCode	00001000h	

You can now answer Question #2!

Answer the questions below

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

practicalmalwareanalysis.com ✓ Correct Answer

How many unique "Imports" are there?

Answer format: * Submit

Task 13 Introduction to Imports

Task 14 Practical Summary

Created by cmmatic Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed!) Users in Room 61,591 Created 1586 days ago

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

File View Tools Help

-Headers Info

Address of Entry Point: 10004E00 Real Image Checksum: 00000104h

Field Name	Data Value	Description
Machine	014Ch	386®
NumberOfSections	00000008h	
TimeDateStamp	4C413E29h	28/09/2010 01:00:25
PointerToSymbolTable	00000000h	
NumberOfSymbols	00000000h	
SizeOfOptionalHeader	00E0h	
Characteristics	210Eh	PE32
Magic	010Bh	6.0
LinkerVersion	0006h	
SizeOfCode	00004000h	
SizeOfInitializedData	0000CA00h	
SizeOfUninitializedData	00000000h	
AddressOfEntryPoint	10004E00h	
BaseOfCode	00001000h	

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows the TryHackMe website with a completed room. The top navigation bar includes links for Dashboard, Learn, Compete, Other, Access Machines, Go Premium, and a user profile icon. A banner at the top right indicates "Room completed (100%)". Below this, a list of tasks is shown, each with a green checkmark and a brief description:

- Task 1: What is the Purpose of Malware Analysis?
- Task 2: Understanding Malware Campaigns
- Task 3: Identifying if a Malware Attack has Happened
- Task 4: Static Vs. Dynamic Analysis
- Task 5: Discussion of Provided Tools & Their Uses
- Task 6: Connecting to the Windows Analysis Environment (Deploy)
- Task 7: Obtaining MD5 Checksums of Provided Files
- Task 8: Now lets see if the MD5 Checksums have been analysed before
- Task 9: Identifying if the Executables are obfuscated / packed

The bottom of the screen shows the Windows taskbar with various pinned icons and system status indicators.

The screenshot shows the TryHackMe website with a completed room. The top navigation bar and user interface are similar to the first screenshot. A central message reads: "achieve this, GL HF!^ If you struggle, revisit the techniques you used above. Moreover, if you're still stuck, visit the TryHackMe Discord!" Below this, a message says: "The file specified for analysis is "ComplexCalculator.exe". It's a simple calculator application. You can leave it up to you to figure out what tool(s) out of what we've learned so far can be used to analyze it." A section titled "Answer the questions below" contains several questions with input fields and buttons for "Correct Answer" or "Hint". One question asks for the MD5 checksum, which is listed as "f5bd8e6dc6782ed4dfa62b8215bcd429". Another asks if VirusTotal reports the file as malicious, with a "Yay" button. A third asks for strings output using Sysinternals "strings" tool. A fourth asks for the last string outputted, with an input field containing "d:h". A fifth asks for the output of PeID, with a result of "Nothing Found". A sixth asks for the output of PEScan, with a result of "Nothing Found". A "Leave Feedback" button is also present. A large "Congratulations!" message is displayed prominently. In the background, a PE Explorer window is open, showing the file structure of a .EXE file named "Task 12\67844C01". The bottom of the screen shows the Windows taskbar with various pinned icons and system status indicators.

Shareable Link - <https://tryhackme.com/r/room/malmalintroductory>

Conclusion

This comprehensive report provides an overview of key aspects related to malware analysis, from its purpose and techniques to practical considerations and tools used in the field. Each task addresses essential components necessary for understanding and combating malware threats effectively.