

DÍA D - EJERCICIO FINAL - CTF ANÁLISIS DE MALWARE

Prerrequisitos

Accede a la plataforma: <https://tryhackme.com>

Una vez identificado en tu cuenta, utiliza el buscador y escribe: "Malware Introductory".

Selecciona el CTF y accede al contenido.

Escenario

El malware es un tema muy frecuente dentro de la ciberseguridad y, lamentablemente, también un elemento recurrente en las noticias a nivel mundial en la

actualidad.

El análisis de malware no solo es una forma de respuesta ante incidentes, sino que también resulta útil para comprender cómo los comportamientos de las

distintas variantes de malware dan lugar a su correspondiente categorización. Esta sala será una introducción práctica a las técnicas y herramientas

utilizadas en el análisis de malware; aunque breve, espero poder ampliar estas técnicas en mayor profundidad en el futuro.

Al analizar malware, es importante tener en cuenta lo siguiente:

Punto de entrada (PoE): Es decir, ¿fue a través de correo no deseado que nuestro filtrado de e-mail no detectó y el usuario abrió el archivo adjunto?

¡Revisemos nuestros filtros de spam y formemos mejor a nuestros usuarios para futuras medidas de prevención!

Indicadores de ejecución: ¿Cuáles son los indicios de que el malware siquiera se ha ejecutado en una máquina? ¿Hay archivos, procesos o quizás algún

intento de comunicación “no ordinaria”?

Comportamiento del malware: ¿Cómo actúa el malware? ¿Intenta infectar otros dispositivos? ¿Cifra archivos o instala algo como una puerta trasera /

herramienta de acceso remoto (RAT)?

Y lo más importante: ¿Podemos, en última instancia, prevenir y/o detectar nuevas infecciones?

Malware Introductory

El reto consiste en completar las siguientes tareas:

Tarea 1. ¿Cuál es el propósito del análisis de malware?

La finalidad de esta tarea es entender el propósito del análisis del malware.

Tarea 1  ¿Cuál es el propósito del análisis de malware?

El malware es un tema muy frecuente en el ámbito de la ciberseguridad y, lamentablemente, suele ser un tema recurrente entre las noticias mundiales actuales. El análisis de malware no solo es una forma de respuesta a incidentes, sino que también es útil para comprender cómo el comportamiento de las variantes de malware resulta en su respectiva categorización. Esta sesión ofrecerá una introducción práctica a las técnicas y herramientas utilizadas en el análisis de malware. Si bien es breve, espero profundizar mucho más en estas técnicas en el futuro.

Al analizar malware, es importante tener en cuenta lo siguiente:

- Punto de Entrada (PoE), es decir, ¿fue a través del spam que nuestro filtro de correo electrónico no detectó y el usuario abrió el archivo adjunto? ;Revisemos nuestros filtros de spam y capacitemos mejor a nuestros usuarios para la prevención futura!
- ¿Cuáles son los indicadores de que se ha ejecutado malware en una máquina? ¿Hay archivos, procesos o algún intento de comunicación inusual?
- ¿Cómo funciona el malware? ¿Intenta infectar otros dispositivos? ¿Cifra archivos o instala algún tipo de puerta trasera o herramienta de acceso remoto (RAT)?
- Lo más importante: ¿podemos prevenir y/o detectar futuras infecciones?

Responda las preguntas a continuación

Ah, ahora lo entiendo un poco...

 No se necesita respuesta  Controlar

Tarea 2. Comprender las campañas de malware.

A "Targeted" attack is just that - targeted. In most cases, malware attacks that occur this way are created for a specific purpose against a specific target. A great example of this type of purpose could be the [DarkHotel](#) malware, whom is designed to steal information such as authentication details from government officials.

Mass Campaign

On the other hand, the "Mass Campaign" classification can be akin to many real life examples, and is the most common type of attacks. The entire purpose of this type of Malware is to infect as many devices as possible and perform whatever it may - regardless of target.

Companies such as Kaspersky to name one, track these campaigns (known as Advanced Persistent Threats (APTs) and often report on their infection rate and indicators, much akin to the real-life spread of a virus from the World Health Organisation (WHO).

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

Tarea 3. Identificar si se ha producido un ataque de malware.

Aquí se pueden visualizar los pasos:

The ultimate process of a malware attack can be broken down into a few broad steps:

1. Delivery
2. Execution
3. Maintaining persistence (not always the case!)
4. Propagation (not always!)

Y mas abajo se encuentran las dos firmas que el malware puede dejar en un host después de un ataque.

Firmas basadas en el host

En términos generales, estos son los resultados de la ejecución y cualquier persistencia realizada por el malware. Por ejemplo, ¿se ha cifrado un archivo? ¿Se ha instalado algún software adicional? Estas son dos de las muchas firmas basadas en el host que es útil conocer para prevenir y evitar futuras infecciones

Firmas basadas en red

En resumen, esta clasificación de firmas es la observación de cualquier comunicación de red que tenga lugar durante la entrega, ejecución y propagación. Por ejemplo en ransomware, ¿dónde ha contactado el malware para los pagos de Bitcoin?

Aquí se muestra la evidencia de la superación del nivel.

These are generally speaking the results of execution and any persistence performed by the Malware. For example, has a file been encrypted? Has any additional software been installed? These are two of many, many host-based signatures that are useful to know to prevent and check against further infection.

Network-Based Signatures

At an 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

?

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

Network-Based Signatures

✓ Correct Answer

?

Tarea 4. Estático vs. Análisis dinámico.

En esta tarea no hay que hacer nada, únicamente comprender las categorías que se utilizan a la hora de analizar el malware.

Existen dos categorías que se utilizan al analizar malware:

- ## 1. Análisis estático



Si bien los métodos y herramientas utilizados para estas dos categorías son muy diferentes, son esenciales para comprender cómo se comporta un malware.

Análisis estático .

En resumen, el "Análisis Estático" se utiliza para obtener una abstracción de alto nivel de la muestra. Con este método, puede ser bastante sencillo determinar si un fragmento de código es "malicioso" (aunque no siempre, ya que se tratará más adelante). En esencia, este método consiste en analizar la muestra en su estado actual, sin ejecutar el código.

El uso de técnicas como el análisis de firmas mediante sumas de comprobación permite realizar un análisis de malware rápido, eficaz (aunque extremadamente breve) y seguro.

Análisis dinámico

Este paso es mucho más complejo y es donde se basa en gran medida la abstracción de la muestra. El «análisis dinámico» implica esencialmente ejecutar la muestra y observar lo que sucede. Por supuesto, esto no es seguro. Si la muestra resulta ser «ransomware», ha perdido sus archivos. Si es capaz de propagarse atravesando una red, genial... Acaba de infectar su red de área local (LAN).

Tenga en cuenta que estas son explicaciones extremadamente simplistas de estas técnicas: hay mucho más involucrado que abordaremos a lo largo de esta serie.

Responda las preguntas a continuación.

¡Entiendo las dos amplias categorías que se emplean al analizar malware potencial!

No se necesita respuesta

✓ Respuesta correcta

Tarea 5. Discusión sobre las herramientas proporcionadas y sus usos.

Lo único que se hace en esta tarea es comprender las herramientas de análisis estático.

Verá que algunas herramientas se superpondrán entre el análisis estático y dinámico:

Herramientas de análisis estático proporcionadas:

C:\ Usuarios\Análisis\Escritorio\ Herramientas\Estático\ Herramientas PE

- Dependency Walker (depende)
 - ID de PE
 - **Explorador de PE**
 - PEview
 - ResourceHacker

C:\Usuarios\Análisis\Escritorio\ Herramientas\Estático\Desmontaje

- IDA Freeware
 - WinDbg

C:\ Usuarios\Análisis\Escritorio\ Herramientas\Sysinternalsuite

- ResourceHacker

C:\ Usuarios\Análisis\Escritorio \Herramientas\Dinámica

Las herramientas enumeradas aquí se utilizarán para tareas futuras, ya que implican depuración, que actualmente está fuera del alcance de esta sala... Sin embargo, se explorarán más adelante en la serie

Responda las preguntas a continuación

Vamos a proceder

No se necesita respuesta

✓ Respuesta correcta

Tarea 6. Conexión al entorno de análisis de Windows (despliegue).

En esta tarea se inicializa la Maquina Virtual que vamos a utilizar para las próximas tareas.

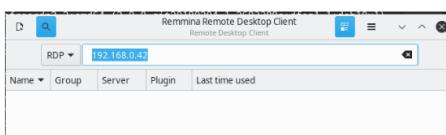
Windows:

- Default Remote Desktop Terminal, replace the IP Address with your **MACHINE_IP**



Linux: Any compatible RDP client such as Remmina: `sudo apt-get install remmina`

Again, replacing the IP address with your **MACHINE_IP**



Answer the questions below

I've logged in!

No answer needed

✓ Correct Answer

Tarea 7. Obtención de sumas de comprobación MD5 de los archivos proporcionados.

Encendemos la maquina virtual desde el ejercicio 6 y nos vamos a la carpeta Tasks luego a Task 7 y ahí en cada uno de los archivos se procede a acceder a sus propiedades luego se procede a entrar a la ventana “File Hashes” y ahí se pueden visualizar los hashes necesarios para superar la prueba.

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

D2778164EF643BA8F44CC202EC7EF157

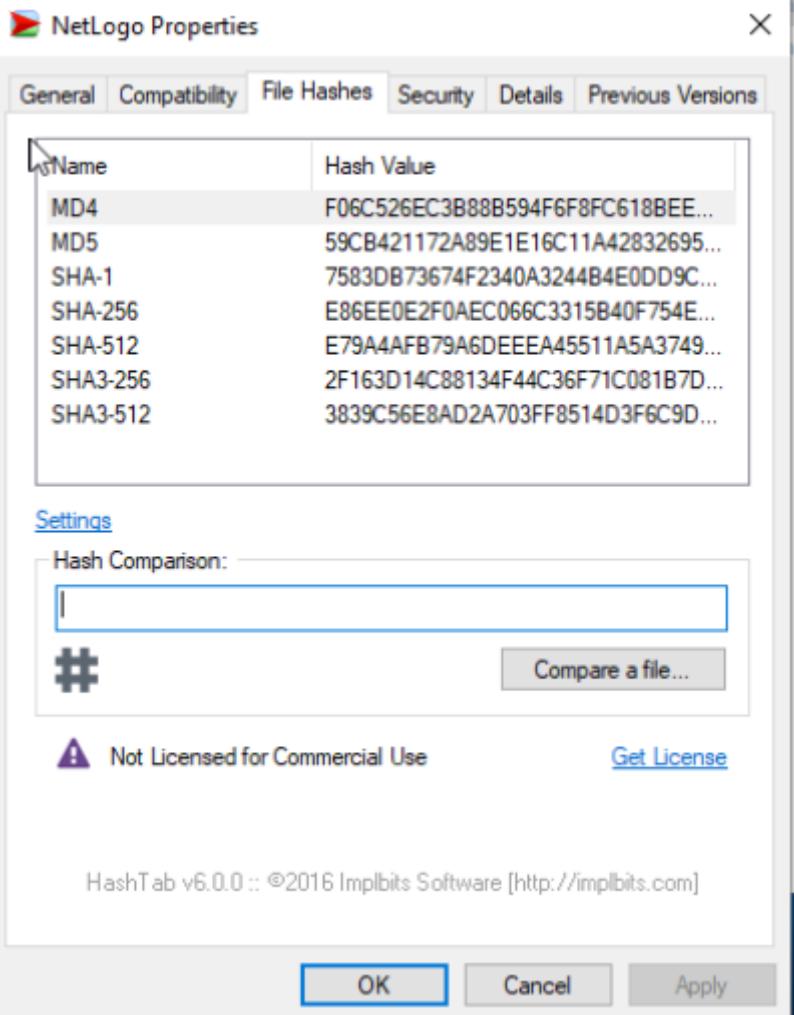
✓ Correct Answer

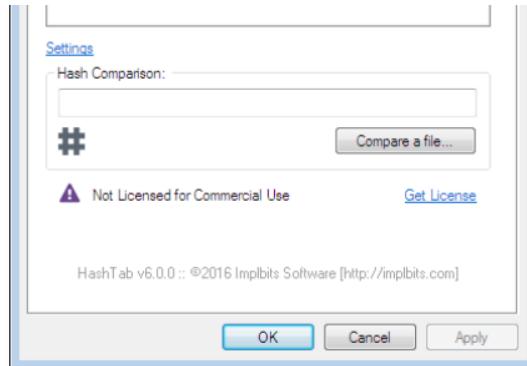
The MD5 Checksum of NetLogo.exe

Check

The MD5 Checksum of vlc.exe

Check





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

D2778164EF643BA8F44CC202EC7EF157

✓ Correct Answer

The MD5 Checksum of Netlogo.exe

59CB421172A89E1E16C11A428326952C

✓ Correct Answer

The MD5 Checksum of vlc.exe

5416BE1B8B04B1681CB39CF0E2CAAD9F

✓ Correct Answer

Tarea 8. Ahora veamos si las sumas de comprobación MD5 se han analizado antes.

Aws.exe no lo califica como malicioso

A screenshot of the VirusTotal analysis page for the file 28b001bb9a72ae7a24242bfab248d767a1ac5dec981c672a3944f7a072375e9a. The page shows a 'Community Score' of 0 / 72. The file is identified as 'File distributed by Microsoft, Linux and others.' The analysis results show a 'Size' of 73.00 KB and an 'Last Analysis Date' of 15 hours ago. The file type is listed as EXE. Below the analysis table, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (29+). A green bar at the bottom encourages users to join the community. At the very bottom, there are links for 'Security vendors' analysis' and 'Do you want to automate checks?'.

Netlogo.exe tampoco lo detecta como malicioso

The screenshot shows the VirusTotal analysis interface for the file e86ee0e2f0aec066c3315b40f754ee25ac3c7d3db7dec20c2e82c8d9f5695536. The file is identified as NetLogo.exe. The community score is 0/72. A note indicates "No security vendors flagged this file as malicious". The file size is 49.00 KB and was last analyzed 2 days ago. The EXE icon is shown. Below the main panel are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. A call-to-action bar at the bottom encourages joining the community.

Vlc.exe tampoco lo muestra como malicioso

The screenshot shows the VirusTotal analysis interface for the file 900021691973aafe47b125d51e1bae5192760e91552dda0c7051226640c0a248. The file is identified as vlc.exe. The community score is 4/72. A note indicates "No security vendors flagged this file as malicious". The file size is 962.70. The EXE icon is shown. Below the main panel are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 5 items). A call-to-action bar at the bottom encourages joining the community.

Aquí se ve como se ha superado el reto.

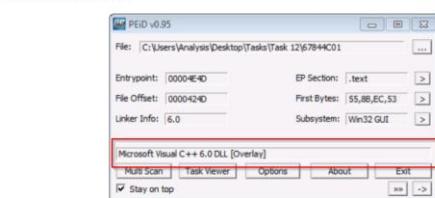
The screenshot shows a challenge task titled "Task 8". The question is "Now lets see if the MD5 Checksums have been analysed before". It asks to look up MD5 Checksums on Virustotal for the file aws.exe. A note says "Outside of the Remote Windows Environment, i.e. Kali or your Windows PC, look up those MD5 "Checksums" on Virustotal to solve this task:". Below the question is a section "Answer the questions below". The first question is "Does Virustotal report this MD5 Checksum / file aws.exe as malicious? (Yay/Nay)". The answer "Nay" is marked as a correct answer. The second question is "Does Virustotal report this MD5 Checksum / file Netlogo.exe as malicious? (Yay/Nay)". The answer "Nay" is marked as a correct answer. The third question is "Does Virustotal report this MD5 Checksum / file vlc.exe as malicious? (Yay/Nay)". The answer "Nay" is marked as a correct answer.

Tarea 9. Identificar si los ejecutables están ofuscados/empaquetados.

Sigue el enlace para ver más información sobre la tarea y las pautas de evaluación.

Herramientas proporcionadas: PEID

Ahora, usando "PEID", identifique el compilador/compactador de los siguientes dos archivos en el directorio "Tareas/Tarea 9" para responder las preguntas.



Ejemplo del uso de PEID para identificar el empaquetador de un archivo. En este caso, se informa como "Microsoft Visual C++ 6.0".

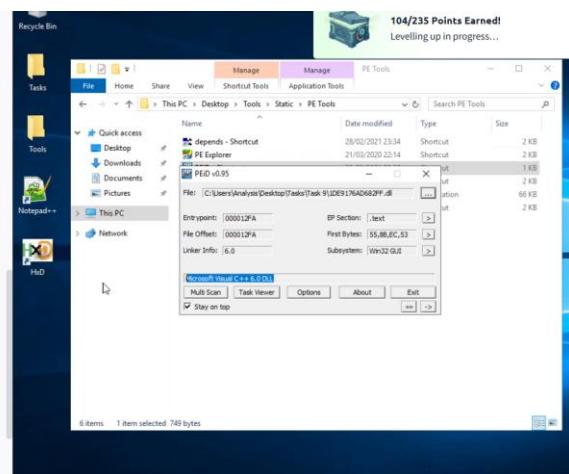
Responda las preguntas a continuación

¿Con qué propone PEID que se empaqueta 1 DE9176AD682FF.dll?

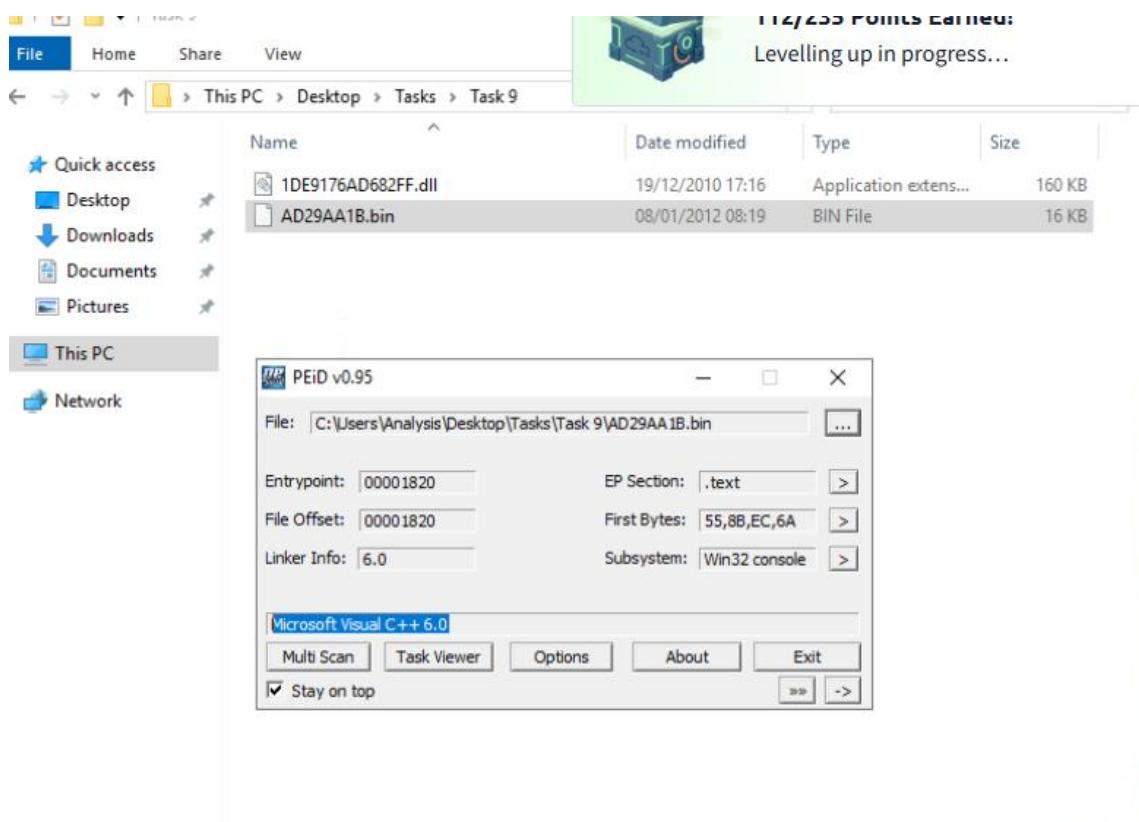
Microsoft Visual C++ 6.0 DLL

✓ Respuesta correcta

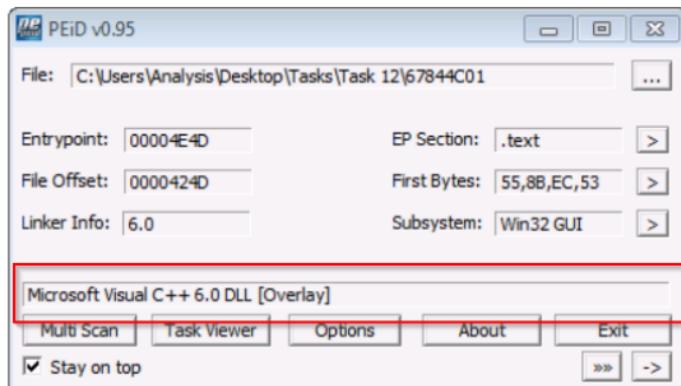
¿Con qué propone PEID empaquetar AD29AA1B.bin?



Para la segunda respuesta al abrir la herramienta esta por defecto filtrando por ejecutables hay que cambiarlo a filtrar por todos para que aparezca el archivo.



Evidencia de superación de los niveles.



Ejemplo del uso de PEiD para identificar el empaquetador de un archivo. En este caso, se informa como "Microsoft Visual C++ 6.0".

Responda las preguntas a continuación

¿Con qué propone PeID que se empaquete 1 DE9176AD682FF.dll?

Microsoft Visual C++ 6.0 DLL

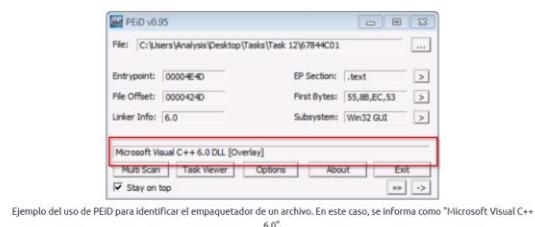
✓ Respuesta correcta



¿Con qué propone PeID empaquetar AD29AA1B.bin ?

Microsoft Visual C++ 6.0

✓ Respuesta correcta



Ejemplo del uso de PEiD para identificar el empaquetador de un archivo. En este caso, se informa como "Microsoft Visual C++ 6.0".

Responda las preguntas a continuación

¿Con qué propone PeID que se empaquete 1 DE9176AD682FF.dll?

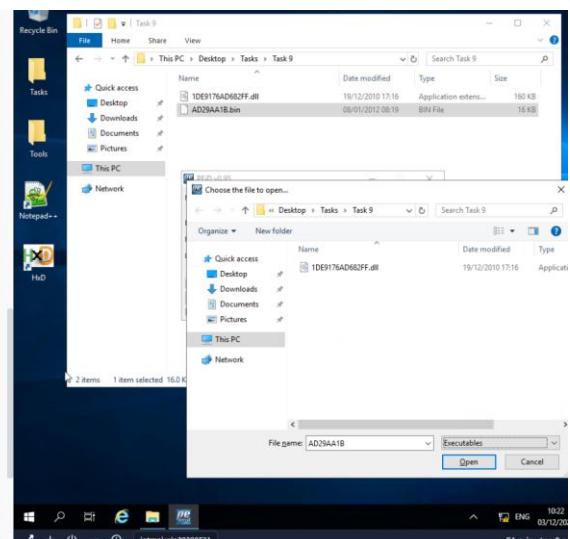
Microsoft Visual C++ 6.0 DLL

✓ Respuesta correcta



¿Con qué propone PeID empaquetar AD29AA1B.bin ?

Comprobar



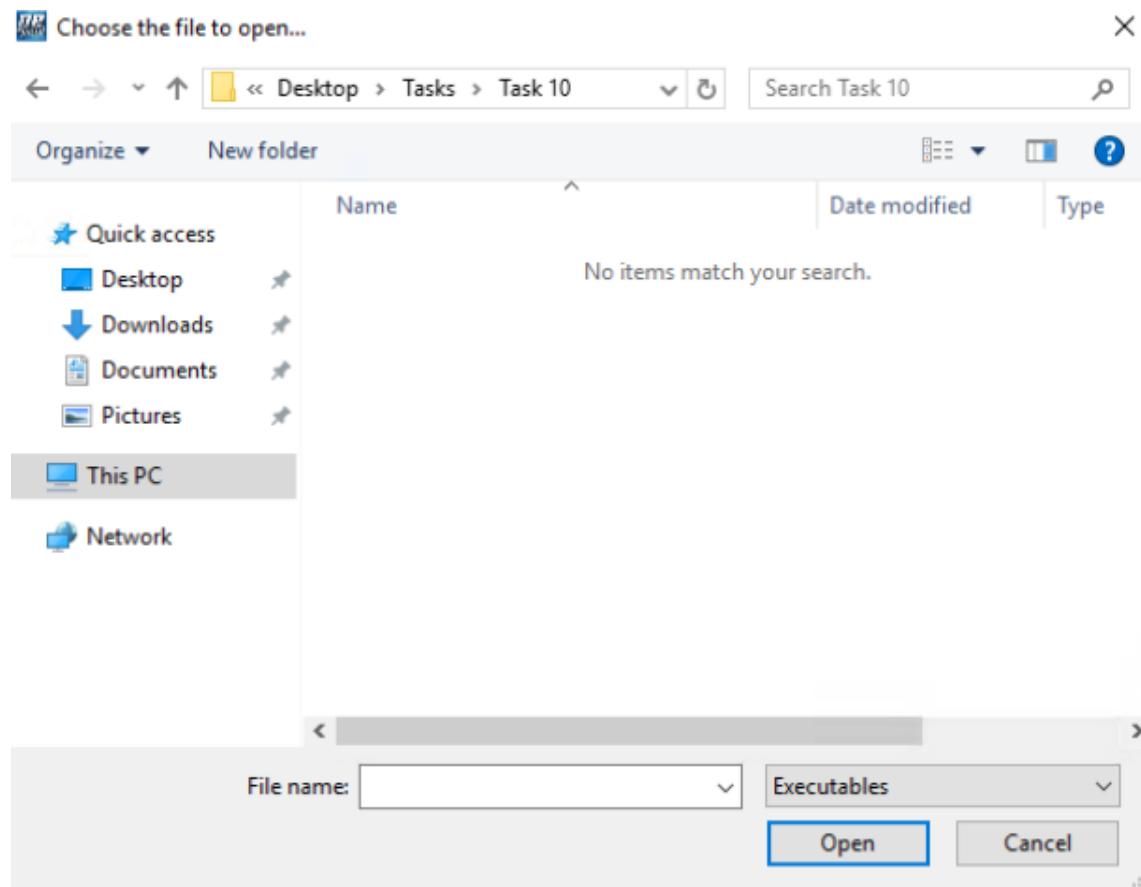
Tarea 10 ¿Qué es la obfuscación/empaquetamiento?

Tarea 11 Visualizando las diferencias entre código empaquetado y no empaquetado

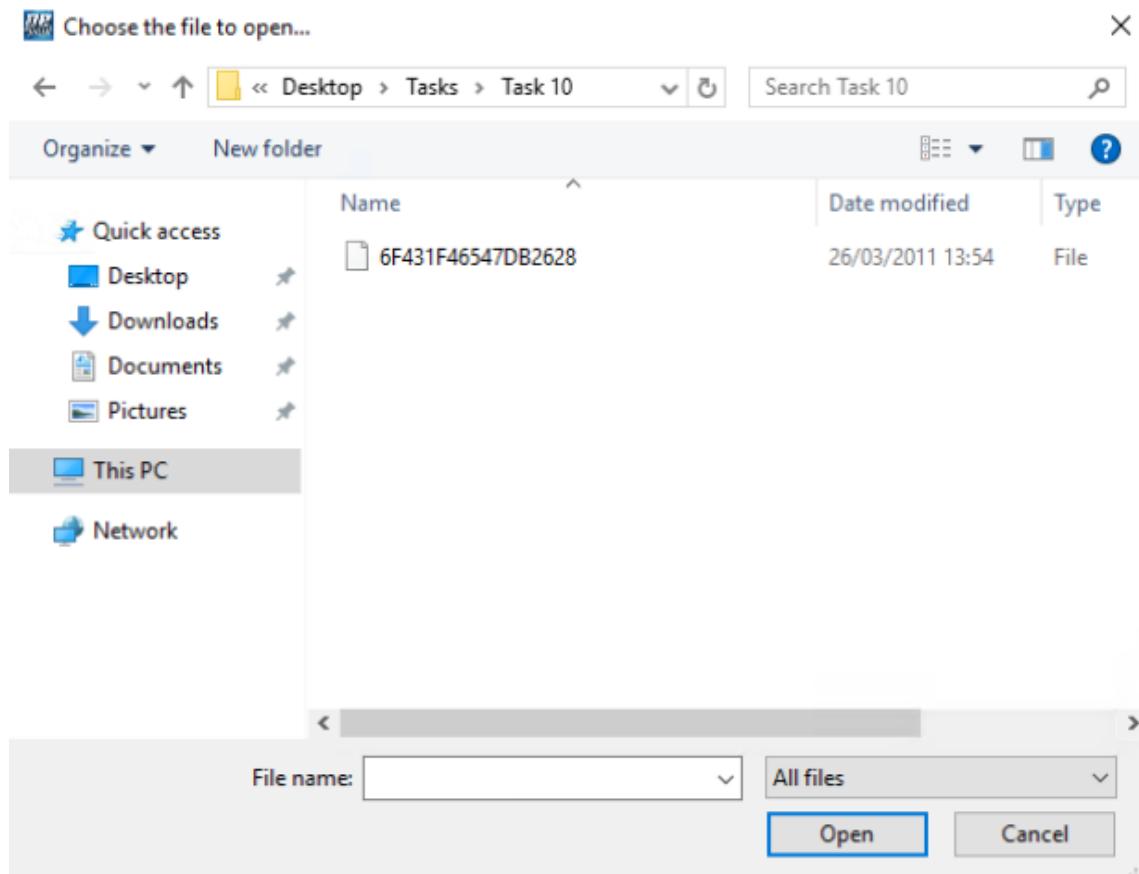
Introducción a las cadenas

Tarea 10. ¿Qué es la ofuscación/empaquetado?.

Abro la herramienta y veo que no aparece ningún archivo en la carpeta de Task 10 y es por el mismo tema de que esta filtrando solo por archivo ejecutables.



Una vez cambiado el filtrado se ve como aparece el archivo que estamos buscando.



Dentro del mismo tenemos la respuesta.

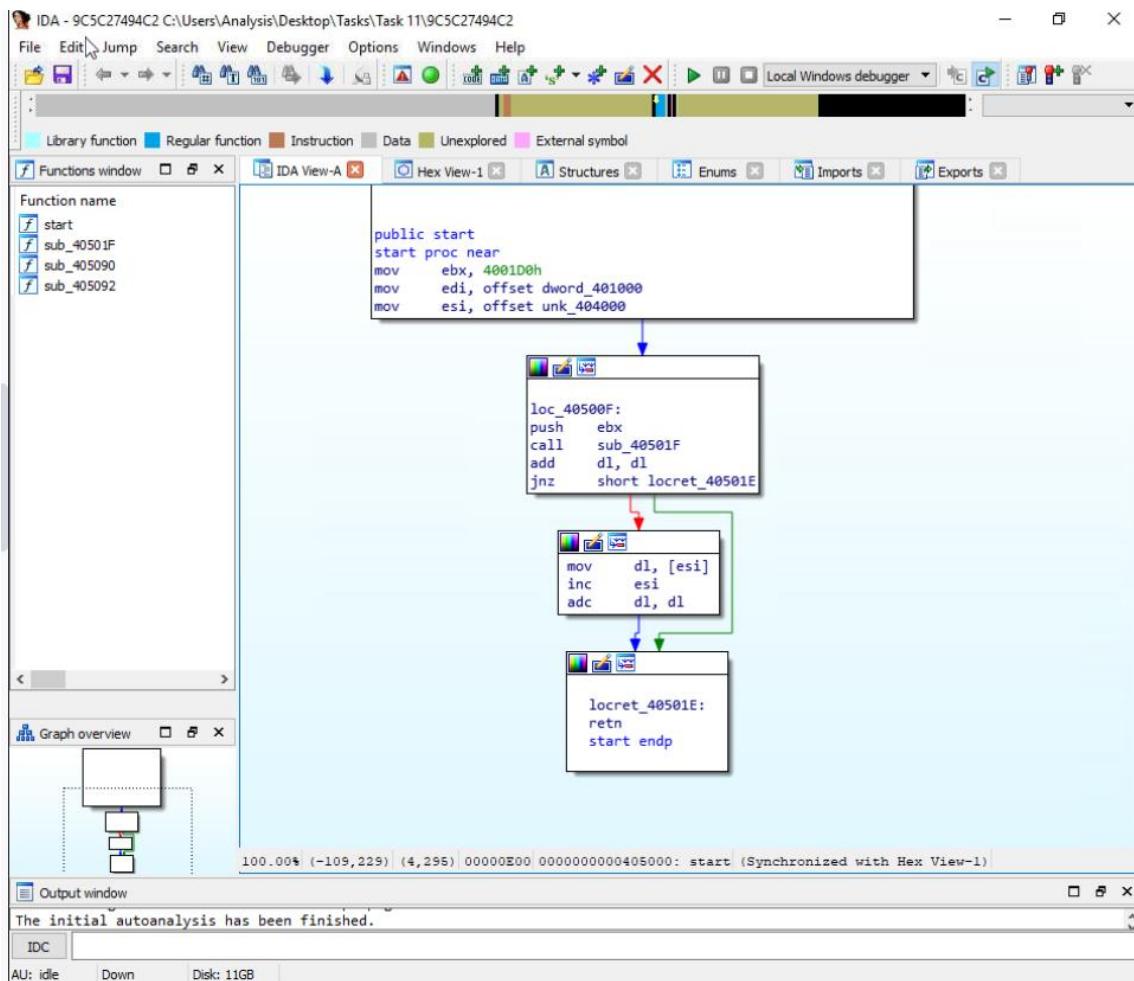
Responda las preguntas a continuación

¿Con qué empaquetador informa PeID que se debe empaquetar el archivo "6F431F46547DB2628"?

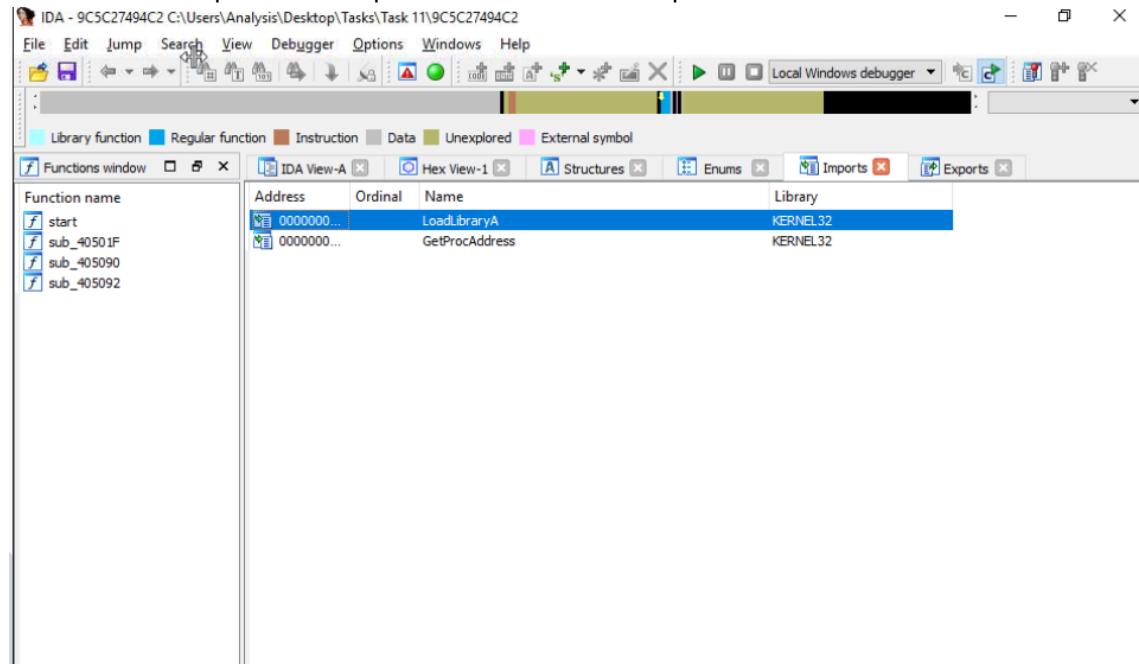
✓ Respuesta correcta

Tarea 11. Visualizando las diferencias entre código empaquetado y no empaquetado.

Abrimos la herramienta iIDA con el archivo del task 11



En la sección Imports se ve que se han intentado importar dos archivos lo cual es extraño



Evidencia de superación del nivel.

Address	Ordinal	Name	Library
00000000		libvlc_add_intf	libvlc
00000000		libvlc_new	libvlc
00000000		libvlc_playlist_play	libvlc
00000000		libvlc_release	libvlc
00000000		libvlc_set_app_id	libvlc
00000000		libvlc_set_user_agent	libvlc
00000000		libvlc_wait	libvlc
00000000		CryptAcquireContextA	ADVAPI32
00000000		CryptGenRandom	ADVAPI32
00000000		CryptReleaseContext	ADVAPI32
00000000		RegOpenKeyExW	ADVAPI32
00000000		RegQueryValueExW	ADVAPI32
00000000		CloseHandle	KERNEL32
00000000		CreateDirectoryW	KERNEL32
00000000		CreateFileW	KERNEL32
00000000		CreateSemaphoreW	KERNEL32
00000000		CreateThread	KERNEL32
00000000		DeleteCriticalSection	KERNEL32
00000000		DeleteFileW	KERNEL32
00000000		DuplicateHandle	KERNEL32
00000000		EnterCriticalSection	KERNEL32
00000000		FindClose	KERNEL32
00000000		FindFirstFileW	KERNEL32
00000000		FindNextFileW	KERNEL32
00000000		FreeLibrary	KERNEL32
00000000		GetCommandLineW	KERNEL32

¿Ves cuánta información hay aquí? El código ofuscado es mucho más difícil de analizar, al menos a nivel estático, ya que se nos presenta muy poca información.

Responda las preguntas a continuación

¡Maldita ofuscación!

No se necesita respuesta

✓ Respuesta correcta

Tarea 12. Introducción a las cadenas ("strings").

Primero abrimos el cmd, vamos a la ruta: cd C:\Users\Analysis\Desktop\Tools\SysinternalsSuite y ejecutamos la herramienta de strings.

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

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.
Rich
.text
.rdata
@.data
.reloc
QQSUVW3
^]
[YY]
```

Y vemos que nos sale la URL que nos pide la respuesta 1

```
Y29ubmVjdA==  
practicalmalwareanalysis.com  
serve.html  
dW5zdXBwb3J0
```

Para la respuesta 2, aquí se puede observar como son 5 las importaciones únicas que hay.

RVA	Name	RVA
100055C2h	KERNEL32.dll	10005034h
100056B0h	ADVAPI32.dll	10005038h
100056CCh	WS2_32.dll	1000503Ch
10005760h	WININET.dll	10005040h
10005886h	MSVCRT.dll	10005044h
		10005048h
		1000504Ch
		10005050h
		10005054h
		10005058h
		1000505Ch

Evidencia de como se ha superado el nivel.

¿Cuál es la URL que se muestra después de usar "strings"?

practicalmalwareanalysis.com

✓ Respuesta correcta

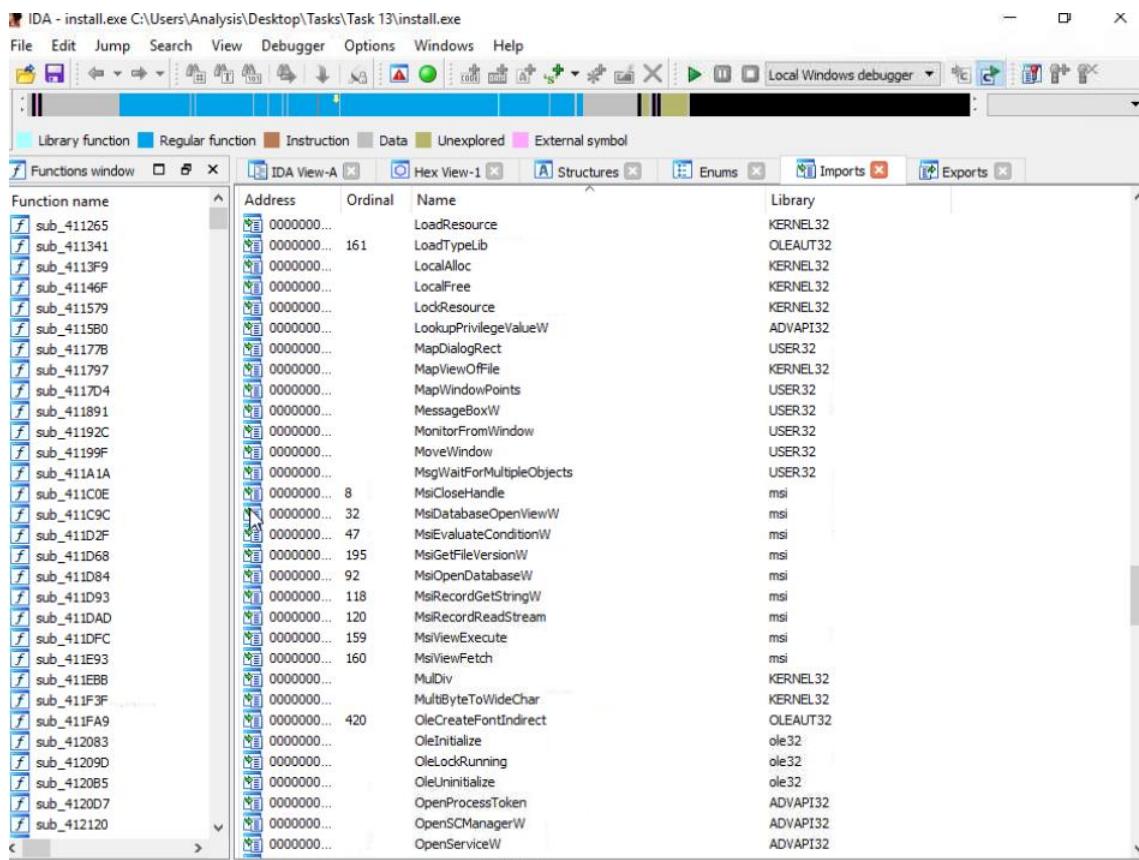
¿Cuántas "Importaciones" **únicas** hay?

5

✓ Respuesta correcta

Tarea 13. Introducción a las importaciones.

Utilizando la herramienta IDA y abriendo el ejecutable install.exe voy a la sección de importaciones y se ve como la librería con nombre msi solo aparece 9 veces.



The screenshot shows the IDA Freeware interface with the 'Imports' tab selected in the top navigation bar. The table lists 9 entries, all of which are from the 'msi' library. The columns are 'Address', 'Ordinal', 'Name', and 'Library'. The 'Library' column shows 'msi' repeated 9 times. The 'Name' column includes functions like LoadResource, LoadTypeLib, LocalAlloc, LocalFree, LockResource, LookupPrivilegeValueW, MapDialogRect, MapViewOfFile, MapWindowPoints, MessageBoxW, MonitorFromWindow, MoveWindow, MsgWaitForMultipleObjects, MsiCloseHandle, MsiDatabaseOpenViewW, MsiEvaluateConditionW, MsiGetFileVersionW, MsiOpenDatabaseW, MsiRecordGetStringW, MsiRecordReadStream, MsiViewExecute, MsiViewFetch, MulDiv, MultiByteToWideChar, OleCreateFontIndirect, OleInitialize, OleLodRunning, OleUninitialize, OpenProcessToken, OpenSCManagerW, and OpenServiceW.

Function name	Address	Ordinal	Name	Library
sub_411265	00000000		LoadResource	KERNEL32
sub_411341	00000000	161	LoadTypeLib	OLEAUT32
sub_4113F9	00000000		LocalAlloc	KERNEL32
sub_41146F	00000000		LocalFree	KERNEL32
sub_411579	00000000		LockResource	KERNEL32
sub_4115B0	00000000		LookupPrivilegeValueW	ADVAPI32
sub_41177B	00000000		MapDialogRect	USER32
sub_411797	00000000		MapViewOfFile	KERNEL32
sub_4117D4	00000000		MapWindowPoints	USER32
sub_411891	00000000		MessageBoxW	USER32
sub_41192C	00000000		MonitorFromWindow	USER32
sub_41199F	00000000		MoveWindow	USER32
sub_411A1A	00000000	8	MsgWaitForMultipleObjects	USER32
sub_411C0E	00000000	32	MsiCloseHandle	msi
sub_411C9C	00000000	47	MsiDatabaseOpenViewW	msi
sub_411D2F	00000000	195	MsiEvaluateConditionW	msi
sub_411D68	00000000	92	MsiGetFileVersionW	msi
sub_411D84	00000000	118	MsiOpenDatabaseW	msi
sub_411D93	00000000	120	MsiRecordGetStringW	msi
sub_411DAD	00000000	159	MsiRecordReadStream	msi
sub_411DFC	00000000	160	MsiViewExecute	msi
sub_411E93	00000000		MsiViewFetch	msi
sub_411EBB	00000000		MulDiv	KERNEL32
sub_411F3F	00000000	420	MultiByteToWideChar	KERNEL32
sub_411FA9	00000000		OleCreateFontIndirect	OLEAUT32
sub_412083	00000000		OleInitialize	ole32
sub_41209D	00000000		OleLodRunning	ole32
sub_4120B5	00000000		OleUninitialize	ole32
sub_4120D7	00000000		OpenProcessToken	ADVAPI32
sub_412120	00000000		OpenSCManagerW	ADVAPI32
	00000000		OpenServiceW	ADVAPI32

Evidencia de superación del ejercicio.

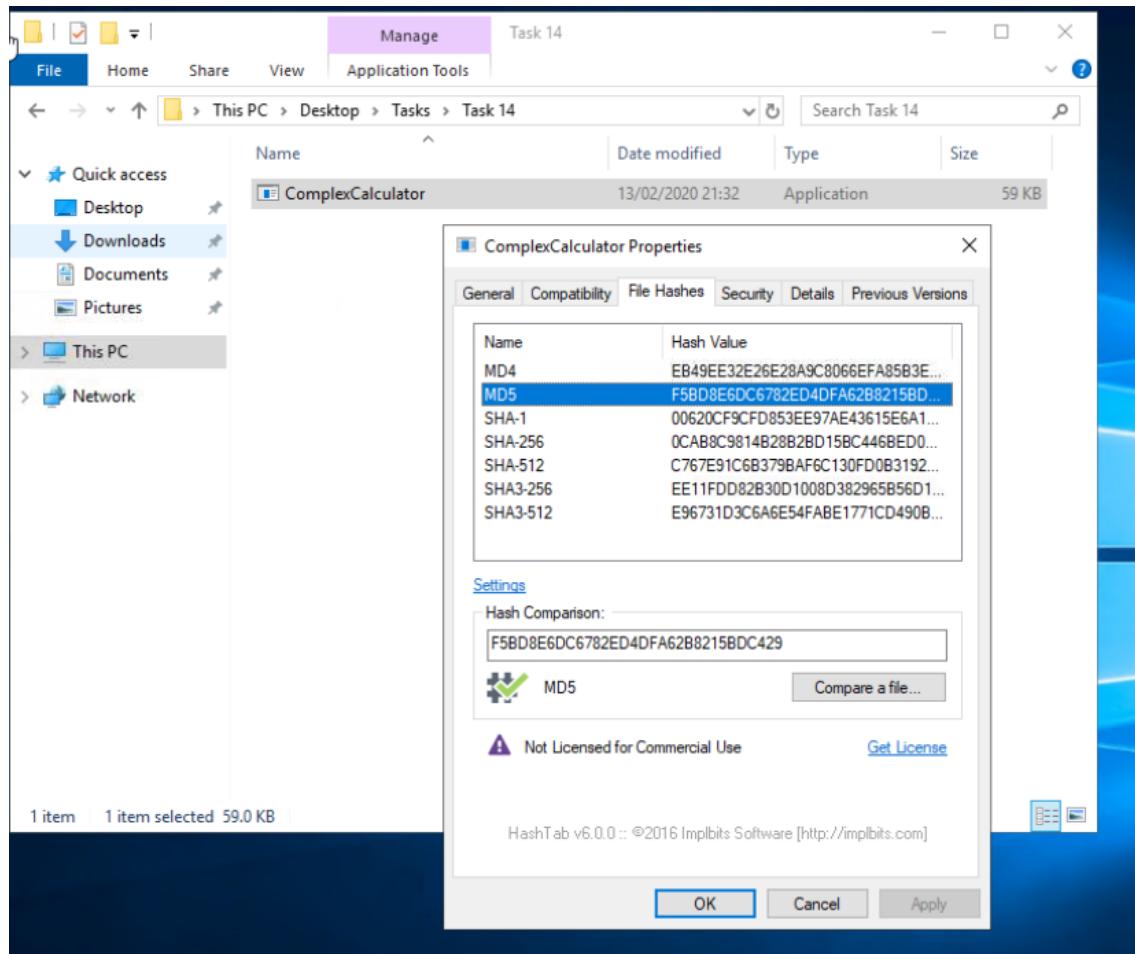
¿Cuántas referencias hay a la biblioteca "msi" en la pestaña "Importaciones" de IDA Freeware para "install.exe"?

9

✓ Respuesta correcta

Tarea 14. Resumen práctico.

Primero me voy a la carpeta 14 al archivo que estamos buscando le hacemos click derecho propiedades y vamos a las secciones de File Hashes y nos aparece el MD5 que estamos buscando.



Después, para la segunda respuesta, vamos a virustotal y pegamos ese MD5 y obtenemos:

The screenshot shows the VirusTotal analysis page for the MD5 hash F5BD8E6DC6782ED4DFA62B8215BDC429. The URL in the address bar is <https://www.virustotal.com/#/file/0cab8c9814b28b2bd15bc446bed045c43498c4b4c54eac62f534c29fc7f7eaab>. The interface shows a red warning icon and the text '2/72 security vendors flagged this file as malicious'. The file details are: Name: ComplexCalculator.exe, Type: PE executable, Size: 59.00 KB, Last Analysis Date: 10 days ago. The analysis results are listed with many tags: peexe, assembly, idle, runtime-modules, detect-debug-environment, direct-cpu-clock-access, checks-user-input, repeated-clock-access. There are also 'Community Score' and 'Reanalyze' buttons.

Con lo cual si detecta que es malicioso.

Para la siguiente respuesta utilizamos la herramienta strings desde cmd:

```
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,
```

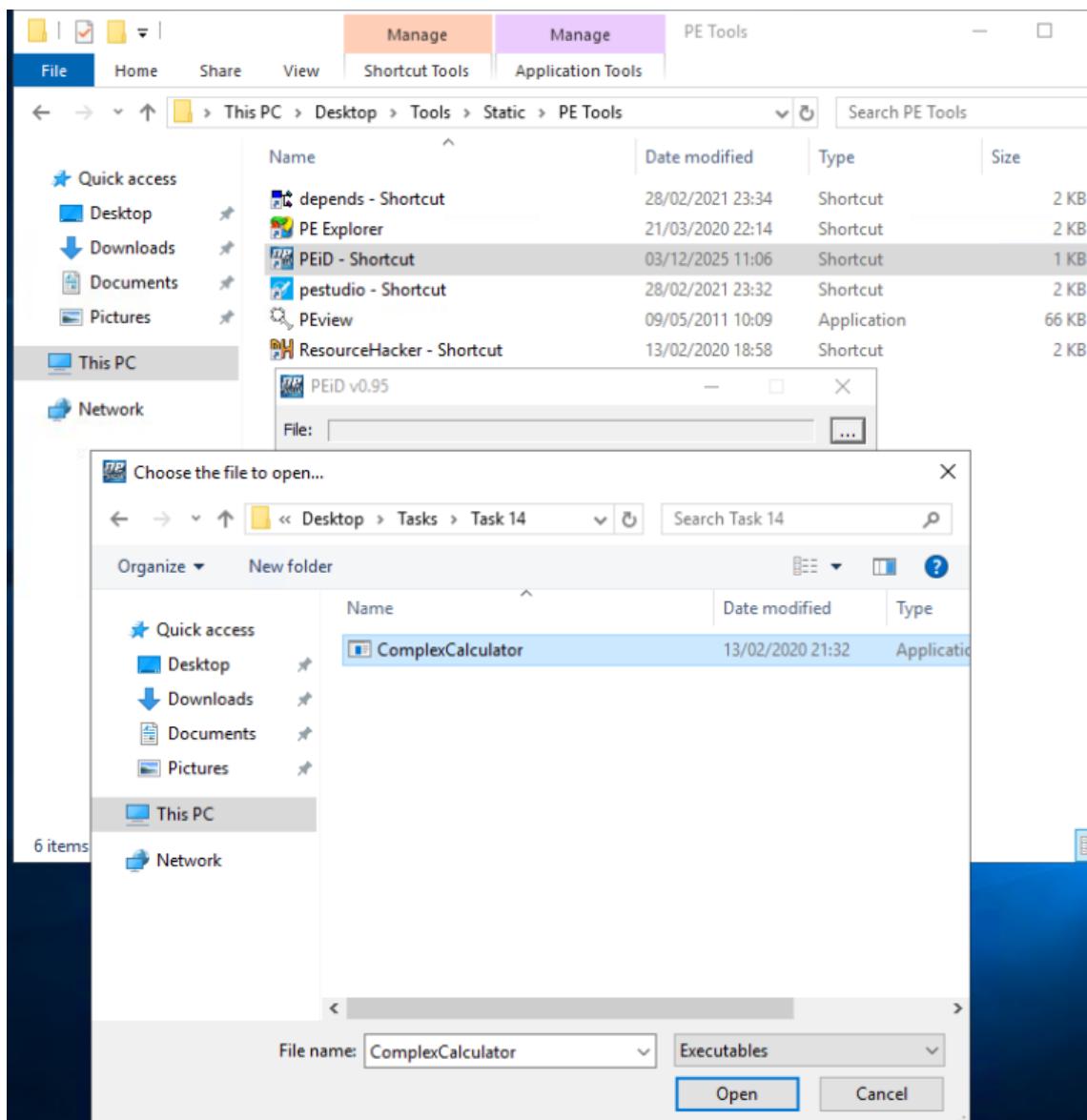
La última cadena usada es: "d:h:" como se puede apreciar en la captura.



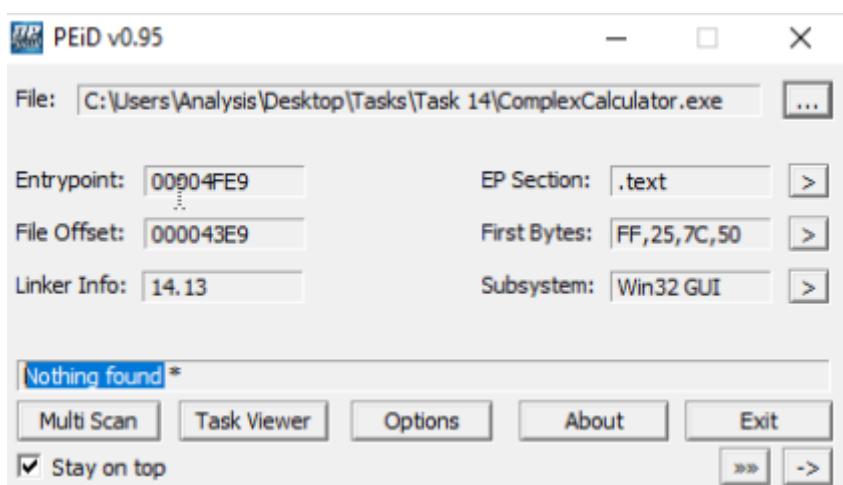
```
1 1&1,12181>1D1J1P1
12282>2
2&3.3B3U3
565_5n5
6w6
7-7;7V7a7
8B8V8]8
:'h:n:
:;;@;e;m;w;
<'</<;<D<I<O<Y<c<s<
=&.=6=A=F=L=V=`=s=x=
>&>P>_>
?9?H?Q?^?v?
0h1l1p1t1
2 2
d:h:

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

Para la siguiente pregunta, abrimos el archivo 14 desde PeID



Se ve la salida de cuando intenta detectar que empaquetador utiliza el archivo.



Evidencia de superación del nivel 14.

Responda las preguntas a continuación

¿Cuál es la suma de comprobación MD5 del archivo?

f5bd8e6dc6782ed4dfa62b8215bdc429

✓ Comprobar

?

¿Virustotal reporta este archivo como malicioso? (Sí/No)

Yay

✓ Comprobar

?

Genera las cadenas utilizando la herramienta "cadenas" de Sysinternals.

¿Cuál es la última cadena generada?

d:h:

✓ Comprobar

?

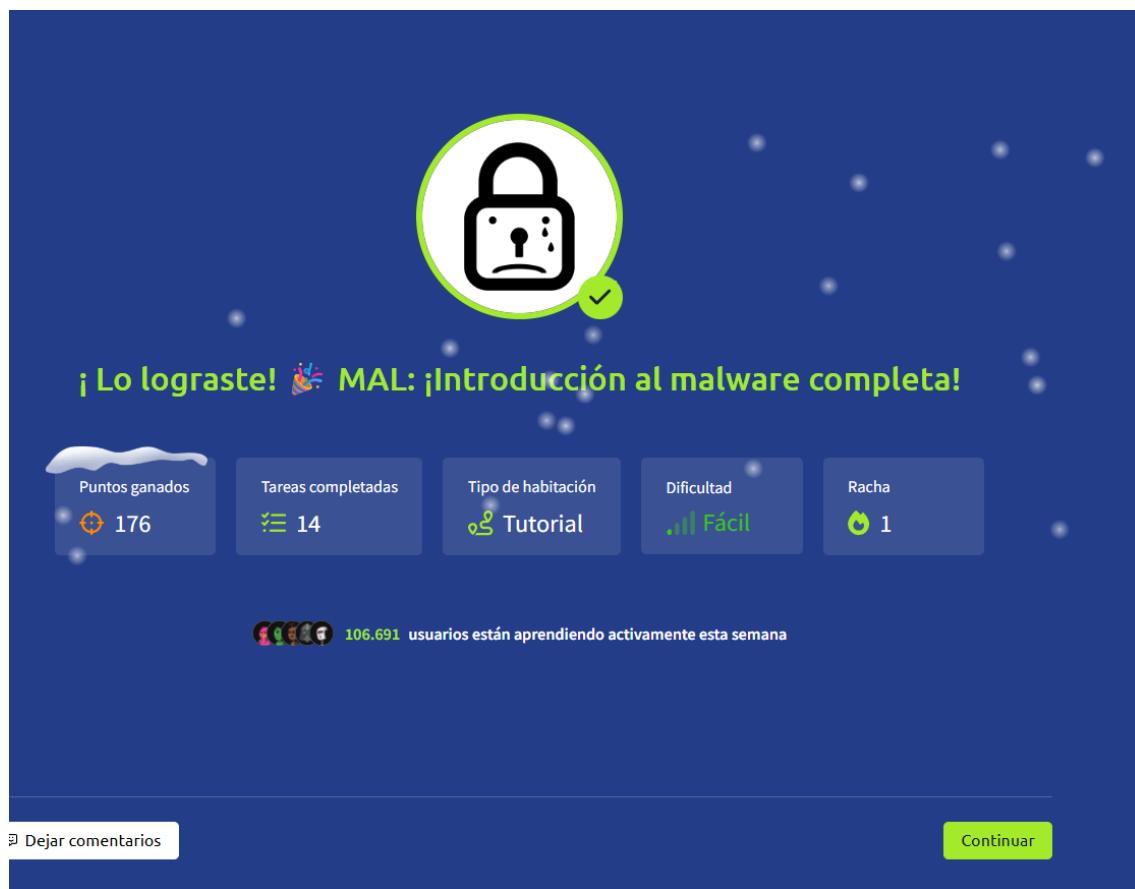
¿Cuál es la salida de PeID cuando intenta detectar qué empaquetador utiliza el archivo?

Nothing Found

✓ Comprobar

?

Aquí se puede visualizar la flag del CTF FINAL.



Hay que documentar el CTF para realizar la entrega individual en moodle. Este debe incluir como mínimo:

Respuesta a cada pregunta formulada.

Explicación de como se ha superado cada prueba y/o nivel.

Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.

Otros retos

Si te ha gustado Análisis de Malware, y quieres más retos para seguir practicando, puedes realizar los siguientes CTF:

TryHackMe Basic Malware RE:

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

TryHackMe Carnage:

<https://tryhackme.com/r/room/c2carnage>

TryHACKMe Dunkle Materie:

<https://tryhackme.com/r/room/dunklematerieptxc9>