

Practica 1

Informe tècnic

TryHackMe - MalBuster



Alumnos: Nicolau Mesalles Campos , Gerard Grau Ruiz , Jordi Barberan Villa ,
Hamza El Haddad Sabri i Oscar Saborido Valdes

Data: 05/05/2025-18/05/2025

Introducció	3
Resultats	4
1. Based on the ARCHITECTURE of the binary, is malbuster_1 a 32-bit or a 64-bit application? (32-bit/64-bit)	4
2. What is the MD5 hash of malbuster_1?	5
3. Using the hash, what is the popular threat label of malbuster_1 according to VirusTotal?	6
trojan.zbot/razy es una etiqueta del malware i el que significa:	6
4. Based on VirusTotal detection, what is the malware signature of malbuster_2 according to Avira?	7
5. malbuster_2 imports the function _CorExeMain. From which DLL file does it import this function?	8
6. Based on the VS_VERSION_INFO header, what is the original name of malbuster_2?	9
7. Using the hash of malbuster_3, what is its malware signature based on abuse.ch?	10
8. Using the hash of malbuster_4, what is its malware signature based on abuse.ch?	11
9. What is the message found in the DOS_STUB of malbuster_4?	12
10. malbuster_4 imports the function ShellExecuteA. From which DLL file does it import this function?	13
11. Using capa, how many anti-VM instructions were identified in malbuster_1?	14
12. Using capa, which binary can log keystrokes?	16
13. What is the MITRE ID of the DISCOVERY technique used by malbuster_4?	17
14. Which binary contains the string GodMode?	18
15. Which binary contains the string Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)?	19
Anàlisi i discussió	20
Conclusions	21

Introducció

Aquesta sala té com a objectiu principal oferir un entorn de pràctica per disseccionar encapçalaments PE (Portable Executable) i realitzar anàlisis estàtiques bàsiques de mostres sospitoses.

En aquest escenari, hem de assumir el rol d'un enginyer invers encarregat d'analitzar mostres de malware detectades pel teu equip de seguretat (SOC), basant-te en les alertes generades per comportaments inusuals dels binaris.

enginyeria inversa: és el procés de desarmar i analitzar un producte existent per entendre com va ser dissenyat i com funciona.

Per tal de treure el màxim profit d'aquesta sala, és era necessari haver completat les següents sales prèvies:

- Introducció a l'anàlisi de malware
- Dissecció dels encapçalaments PE
- Anàlisi estàtica bàsica

Context de l'escenari

Fem la funció de enginyer d'anàlisi de malware dins la teva organització. El nostre equip col·labora estretament amb el SOC, que és el responsable de monitorar i respondre a amenaces en temps real.

Recentment, un analista del SOC ha detectat binaris desconeguts amb comportaments sospitosos. Hem d'analitzar aquestes mostres i proporcionar conclusions que ajudin a identificar la naturalesa del fitxer i determinar la millor manera de mitigar la possible amenaça.

Per dur a terme l'anàlisi, disposem de dues màquines virtuals preparades específicament per a aquesta tasca:

- FLARE VM (Màquina virtual Windows)
- REMnux VM (Màquina virtual Linux)

Les mostres que cal analitzar es troben a:
C:\Users\Administrator\Desktop\Samples

Excepte les últimes 2 tasques hem utilitzat la màquina FLARE VM (Màquina virtual Windows) però es pot utilitzar els 2 sistemes operatius per fer tota la pràctica.

Resultats

1. Based on the ARCHITECTURE of the binary, is malbuster_1 a 32-bit or a 64-bit application? (32-bit/64-bit)

Hem utilitzat la app de windows pestudio per analitzar el malware i veure si està dissenyat per dispositius de 32 bits o 64 bits.

Aquesta informació és important ja que un malware de 64 bits no funcionarà en sistemes operatius de 32 bits i un malware de 32 bits no pot executar-se en un sistema de 64 bits que no tingui suport per a aplicacions de 32 bits (la majoria de sistemes moderns sí que en tenen).

La informació l'hem obtingut en obrir l'arxiu de malbuster_1 en el pestudio, observant l'apartat cpu ens adonem que ens diu de quants bits és, en aquest cas és 32-bit,

The screenshot shows the Pestudio 9.22 interface. The left pane displays the file's structure, with the 'cpu' property highlighted in the 'optional-header (GUI)' section. The right pane shows the 'property value' table, where the 'cpu' property is set to '32-bit' and is highlighted with a red box. The 'file-type' is 'executable' and the 'subsystem' is 'GUI'.

property	value
md5	4348DA65E4AE6472C7F97D6DD8AD8E
sha1	8BF60EEA83C34EC9DE2359219978B8805F2629E3
sha256	000415D1C7A7A838BA2EF00874E352E8B43A57E2F98539B5908803056F883176
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 40 00 00 00
first-bytes-text	M Z@
file-size	155648 (bytes)
entropy	6.719
imphash	wait...
signature	n/a
entry-point	55 8B EC 83 EC 14 A1 24 27 98 00 56 57 FF 70 20 33 FF 57 68 E8 13 98 00 89 7D F8 FF
file-version	wait...
description	n/a
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	0x49288BEB (Sat Nov 22 14:47:07 2008)
debugger-stamp	
resources-stamp	wait...
import-stamp	wait...
exports-stamp	wait...
version-stamp	wait...
certificate-stamp	wait...

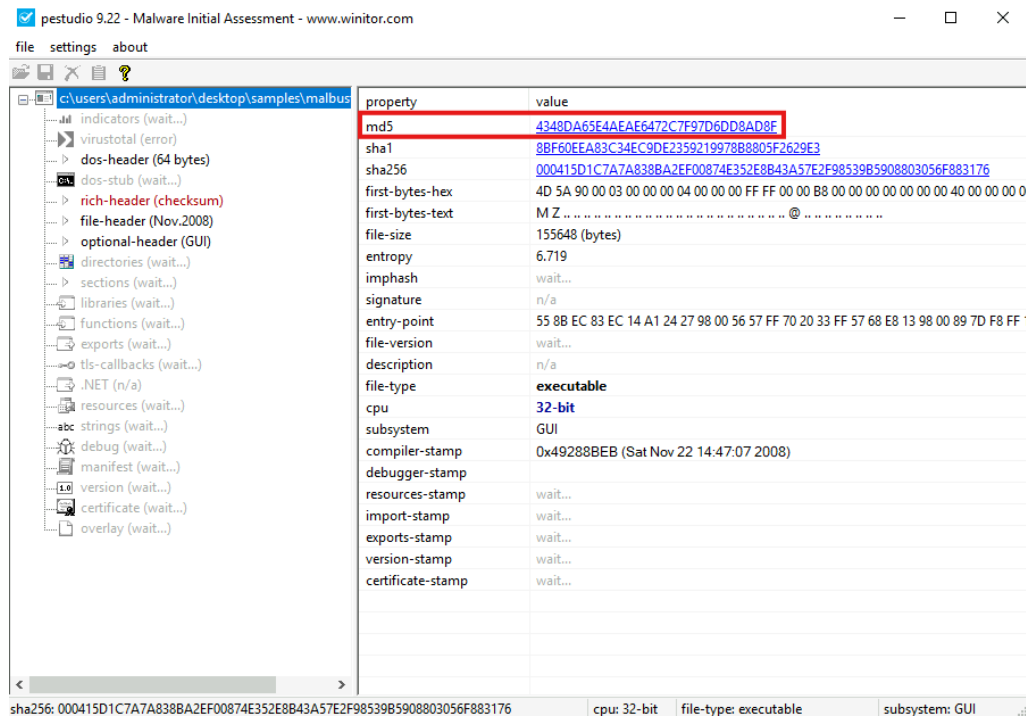
sha256: 000415D1C7A7A838BA2EF00874E352E8B43A57E2F98539B5908803056F883176 cpu: 32-bit file-type: executable subsystem: GUI

2.What is the MD5 hash of malbuster_1?

Cada arxiu té un hash únic, això permet identificar i comparar mostres de malware ràpidament, fins i tot entre analistes o laboratoris diferents.

Es pot cercar l'MD5 en bases de dades públiques com VirusTotal o Malware Bazaar per veure si ja ha sigut analitzat.

Per trobar l'MD5, en la mateixa aplicació que abans i el mateix arxiu obert, en la columna de “property” ens adonem que el tenim a la primera fila, amb el valor del hash a la seva dreta.



Hash md5: 4348da65e4aeae6472c7f97d6dd8ad8f

3. Using the hash, what is the popular threat label of malbuster_1 according to VirusTotal?

Hem cercat el hash aconseguit anteriorment de l'arxiu malbuster_1 en VirusTotal, podem observar que 59/72 proveïdors de seguretat han marcat aquest fitxer com a maliciós

trojan.zbot/razy es una etiqueta del malware i el que significa:

- Trojan → És un troià, un tipus de malware que es fa passar per programari legítim però que executa accions malicioses.
- zBot (Zeus Bot) → Fa referència a la família Zeus, un troià bancari molt conegut, utilitzat per robar credencials, informació financera i injectar codi en navegadors.
- razy → És una altra família de malware. Razy sovint es propaga com una extensió de navegador maliciós o mitjançant carregadors, i pot modificar pàgines web, injectar publicitat o robar criptomonedes.

Una entrada trojan.zbot/razy com en una eina com VirusTotal vol dir que la mostra:

- És un troià
- Té components de Zeus/Zbot (ex. keylogger, robatori de dades)
- Te funcions relacionades amb la família Razy (manipulació del navegador, mineria, adware, etc.).

59 / 72
Community Score

59/72 security vendors flagged this file as malicious

000415d1c7a7a838ba2ef00874e352eb43a57e2f98539b5908803056f883176
000415d1c7a7a838ba2ef00874e352eb43a57e2f98539b5908803056f883176.bin

Size: 152.00 KB
Last Analysis Date: 6 days ago
EXE

peexe detect-debug-environment corrupt overlay checks-user-input spreader

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 17

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

Popular threat label **trojan.zbot/razy** Threat categories trojan pua spyware Family labels zbot razy smrl

Security vendors' analysis Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Worm/Win32.IRCBot.C136977
Alibaba	Trojan/PSW/Win32/ShellCode.954c5755	AliCloud	Trojan(spy)/Win/Zbot.RL8PHU
ALYac	Gen.Variant.Razy.447136	Antiy-AVL	Trojan(PSW)/Win32.Zbot
Arcabit	Trojan.Razy.D6D2A0	Arctic Wolf	Unsafe

Popular threat label **trojan.zbot/razy** Threat categories trojan pua spyware Family labels zbot razy smrl

4. Based on VirusTotal detection, what is the malware signature of malbuster_2 according to Avira?

Igual que la part anterior hem cercat a VirusTotal però aquest cas amb el hash de malbuster_2

En aquesta captura que l'antivirus alemany Avira (no cloud) ha detectat que malbuster_2 es un troya.

- Hash md5: TR/Spy.Zbot.usvqc
- TR/: abreviatura de Trojan, és a dir, un troià.
- Spy: indica que és un spyware, o sigui, un programari dissenyat per espiar l'activitat de l'usuari, sovint robant informació com contrasenyes, dades bancàries o altres dades sensibles.
- Zbot: fa referència a la família de malware coneguda com Zeus Botnet (Zbot), un dels troians bancaris més coneguts.
- usvqc: aquest sufix sol ser un identificador únic dins del sistema de detecció d'Avira. No té una traducció clara, però serveix per distingir variants concretes del malware.

58 / 72
Community Score

58/72 security vendors flagged this file as malicious

Reanalyze Similar More

ace3a5e5849c1c00760dfe67add397775f5946333357f5f8dee25cd4363e36b6
7.JyP.exe
Size: 835.00 KB
Last Analysis Date: 6 days ago
EXE

peexe persistence runtime-modules detect-debug-environment long-sleeps checks-user-input assembly direct-cpu-clock-access spreader cve-2014-3931 exploit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

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

Popular threat label trojan.msil/agenttesla Threat categories trojan Family labels msil agenttesla variadic

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan:Win.PWSX-gen.C4565347	Alibaba	Trojan:MSIL/AgentTesla.4c64d230
AliCloud	Trojan:MSIL/AgentTesla.CFY2XJC	Arcabit	Trojan.Variadic.A.304.2
Arctic Wolf	Unsafe	Avast	Win32:MalwareX-gen [Pws]
AVG	Win32:MalwareX-gen [Pws]	Avira (no cloud)	HEUR/AGEN.1306860

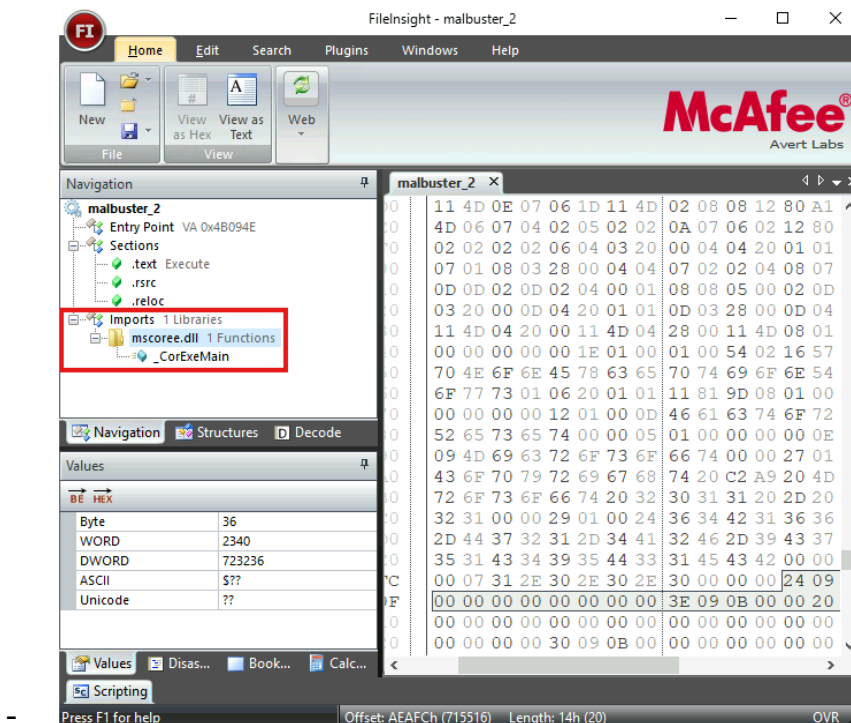
5. malbuster_2 imports the function _CorExeMain. From which DLL file does it import this function?

Per trobar des de quin DLL s'importa la funció _CorExeMain hem obert l'arxiu malbuster_2 en Fileinsight, una eina d'anàlisi gratuïta proporcionada per a investigadores de seguretat.

_CorExeMain és el punt d'entrada de les aplicacions .NET que s'encarrega de posar en marxa el CLR (entorn que interpreta i executa codi).

mscorlib.dll és la biblioteca que conté aquesta funció i que permet inicialitzar i executar aplicacions .NET dins de Windows.

CorExeMain i mscorlib.dll poden ser utilitzats pel malware, sobretot si aquest està desenvolupat amb tecnologies .NET perquè si un malware està escrit en C#, VB.NET o un altre llenguatge .NET, automàticament dependrà d'ells.

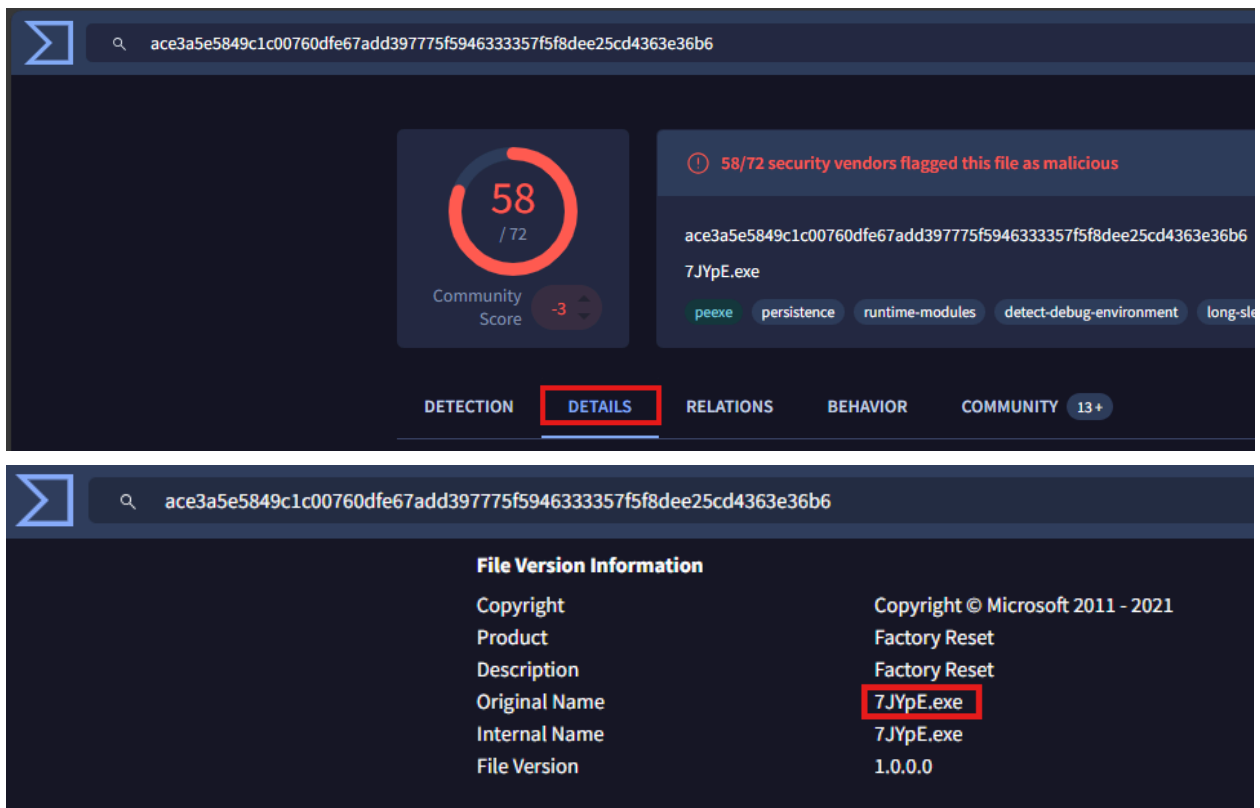


6. Based on the VS_VERSION_INFO header, what is the original name of malbuster_2?

També a VirusTotal la búsqueda del Hash de malbuster_2, si anem a “**DETAILS**” podem veure el nom original del executable del malware.

Saber el nom original del malware és útil per a la detecció, investigació i resposta davant d'un incident de seguretat.

Aquesta informació pot ajudar tant als analistes de seguretat com als sistemes automàtics a identificar, rastrejar i neutralitzar l'amenaça de manera més eficaç.



The image shows two screenshots of the VirusTotal web interface. The top screenshot displays the main file analysis page for the hash `ace3a5e5849c1c00760dfe67add397775f5946333357f5f8dee25cd4363e36b6`. It shows a community score of 58/72, a status of "58/72 security vendors flagged this file as malicious", and the filename `7JYpE.exe`. The bottom screenshot shows the "DETAILS" tab, specifically the "File Version Information" section. This section contains a table with the following data:

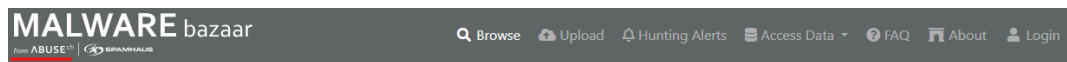
File Version Information	
Copyright	Copyright © Microsoft 2011 - 2021
Product	Factory Reset
Description	Factory Reset
Original Name	7JYpE.exe
Internal Name	7JYpE.exe
File Version	1.0.0.0

7. Using the hash of malbuster_3, what is its malware signature based on abuse.ch?

En aquest cas ens demana que busquem la signatura del malware malbuster_3 basada en abuse.ch.

VirusTotal no busca informació de l'antivirus que busquem, hi ha una altre pàgina que es MALWARE bazaar DATABASE on utilitzant el hash del malware podem buscar el que ens demana.

En aquesta captura es veu que el sistema identifica la mostra com una amenaça coneguda, proporcionant una signatura concreta. Aquesta signatura ajuda a classificar el comportament del malware i, en entorns reals, permet aplicar mesures de detecció més eficients basades en la seva família o tècnica d'infecció.



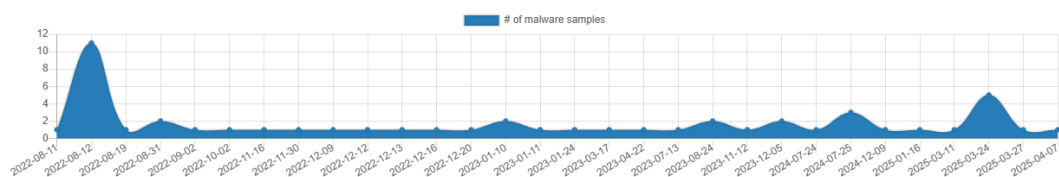
Browse / Signature

MalwareBazaar Database

MalwareBazaar tries to identify the malware family (signature) of submitted malware samples. A malware sample can be associated with only one malware family. The page below gives you an overview on malware samples that MalwareBazaar has identified as [TrickBot](#).

Database Entry

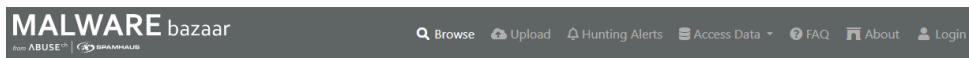
Signature:	TrickBot Alert
Firstseen:	2020-02-03 09:54:52 UTC
Lastseen:	2025-04-07 04:19:55UTC
Malware samples:	5'419



8. Using the hash of malbuster_4, what is its malware signature based on abuse.ch?

Utilitzant el hash de malbuster_4, obtenible de la mateixa manera que els anteriors, podem utilitzar-lo per buscar la signatura en Malware Bazaar Database com s'observa en la següent imatge, la qual mostra el resultat de la cerca.


La signatura retornada per abuse.ch permet relacionar-la amb una família específica i comprendre millor les seves funcionalitats potencials.




MalwareBazaar Database

You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpus, you can do so through either using the [web upload](#) or the [API](#).


495
Submissions (past 24 hours)


Mirai
Most seen malware family (past 24 hours)


917'805
Malware samples in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

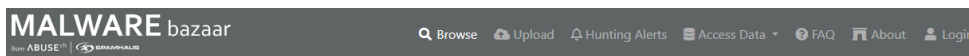
Browse Database

Search

Search Syntax ⓘ

Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2020-07-05 20:48	00272dd639402fa76db4...	<input type="checkbox"/> exe	Zloader	dll Zloader	Racco42	



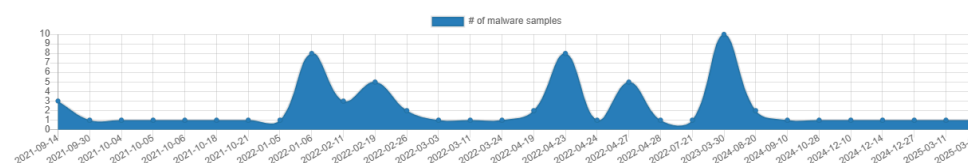
Browse / Signature

MalwareBazaar Database

MalwareBazaar tries to identify the malware family (signature) of submitted malware samples. A malware sample can be associated with only one malware family. The page below gives you an overview on malware samples that MalwareBazaar has identified as **Zloader**.

Database Entry

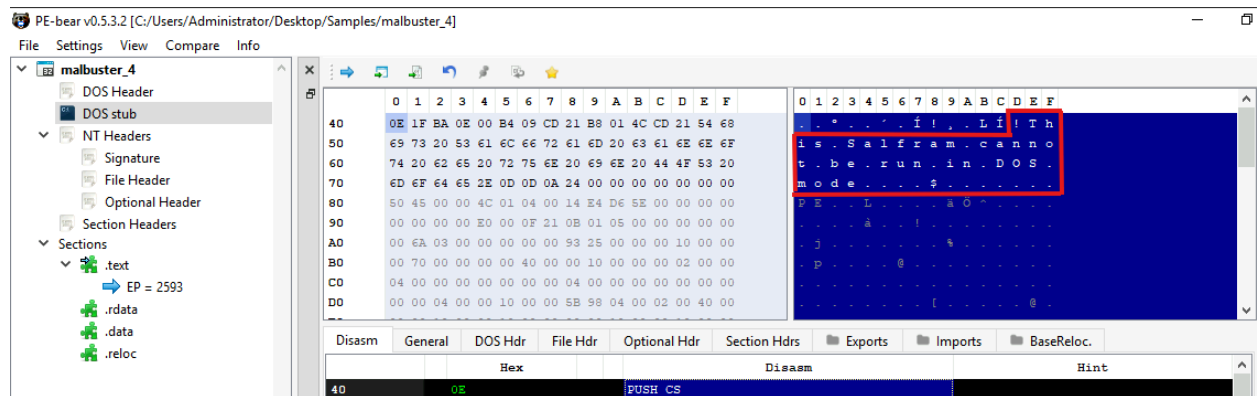
Signature:	Zloader
Firstseen:	2020-03-27 08:05:10 UTC
Lastseen:	2025-03-13 13:36:12UTC
Malware samples:	1'329



9. What is the message found in the DOS_STUB of malbuster_4?

Ara utilitzant PE-bear podem aconseguir un missatge al obrir el fitxer malbuster_4 i anar a la secció DOS stub, com es pot observar en la imatge, el missatge present a la secció DOS_STUB de malbuster_4.

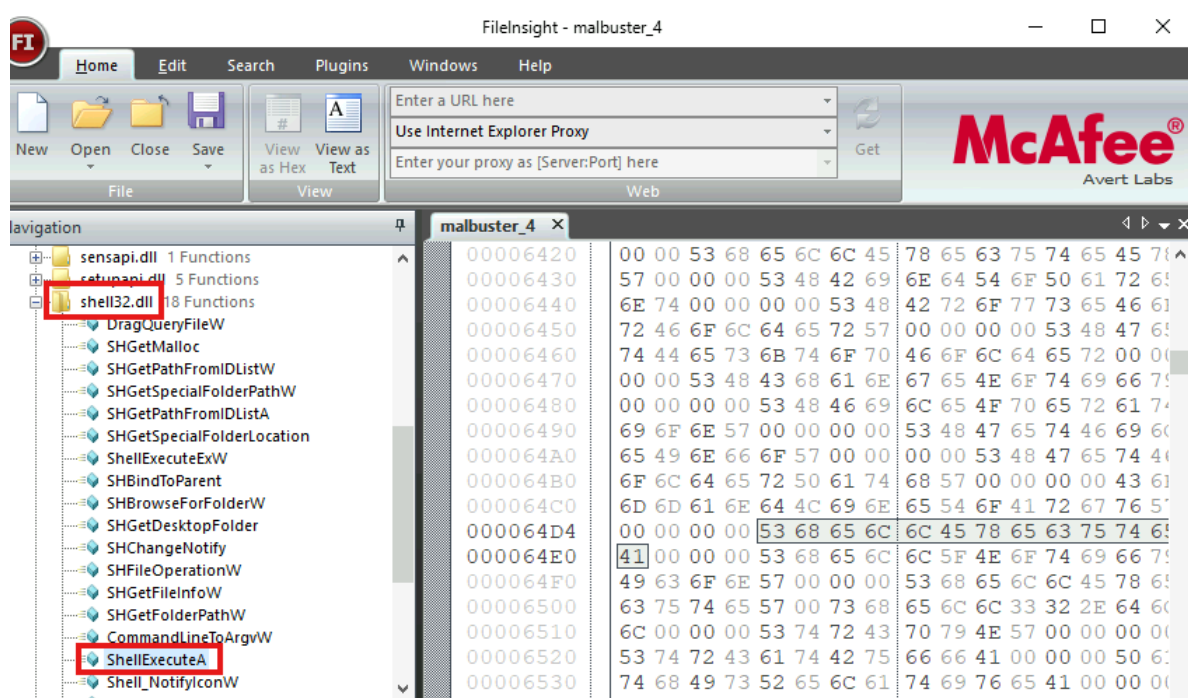
Aquest missatge és típic dels executables de Windows i serveix per confirmar que no es pot executar en entorns DOS antics.



10.malbuster_4 imports the function ShellExecuteA. From which DLL file does it import this function?

Aquí hem tornat a buscar des de quin DLL s'importava una funció, com hem fet anteriorment, hem utilitzat FileInsight per trobar des d'on s'executava la funció ShellExecuteA.

Com es mostra en l'imatge, malbuster_4 importa la funció ShellExecuteA des de la DLL SHELL32.DLL. Aquesta funció és sovint utilitzada per malware per executar fitxers o comandes externes sense interacció de l'usuari.



11.Using capa, how many anti-VM instructions were identified in malbuster_1?

Utilitzant CAPA, hem analitzat la mostra malbuster_1 per trobar quantes instruccions d'anti-VM havien en l'arxiu.

Per veure la informació de CAPA, primer hem de executar l'aplicació tot seguit en el nostre cas hem d'executar la següent comanda:

```
capa.exe Samples\malbuster_1
```

Samples\malbuster_1 -> direcció on es troba el malware.

Podem observar en la imatge com l'eina capa detecta 3 instruccions anti-VM dins de malbuster_1. Aquestes instruccions indiquen mecanismes d'evasió per evitar ser analitzat en entorns controlats o de sandboxing.

```
C:\Windows\system32\cmd.exe - Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

FLARE Mon 05/12/2025 0:39:05.47
C:\Users\Administrator>cd Desktop

FLARE Mon 05/12/2025 0:39:10.59
C:\Users\Administrator\Desktop>capa.exe Samples\malbuster_1

loading : 100%|██████████████████████████████████████████████████| 703/703 [00:00<00:00, 803.49 rules/s]
matching: 100%|██████████████████████████████████████████████████| 412/412 [00:19<00:00, 20.61 functions/s, skipped 4 library functions (0%)]
```

Després d'executar la comanda podem observar un munt d'informació, en el nostre cas ens demana que contem quants anti-VM (anti Virtual Machine) hi ha al malware `malbuster_1`. el que fa és detectar si el codi està sent executat per una màquina virtual i canviar el seu comportament en cas que si.

ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Obfuscated Files or Information T1027
	Virtualization/Sandbox Evasion::System Checks T1497.001
MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Virtual Machine Detection [B0009]
COMMUNICATION	HTTP Communication::Read Header [C0002.014]
CRYPTOGRAPHY	Encrypt Data::RC4 [C0027.009]
	Generate Pseudo-random Sequence [C0021]
	Generate Pseudo-random Sequence::Mersenne Twister [C0021.005]
	Generate Pseudo-random Sequence::RC4 PRGA [C0021.004]
DATA	Checksum::CRC32 [C0032.001]
	Encode Data::XOR [C0026.002]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]
DISCOVERY	Code Discovery::Enumerate PE Sections [B0046.001]
CAPABILITY	NAMESPACE
reference anti-VM strings	anti-analysis/anti-vm/vm-detection
check HTTP status code (2 matches)	communication/http/client
hash data with CRC32	data-manipulation/checksum/crc32



Administrator: Co...

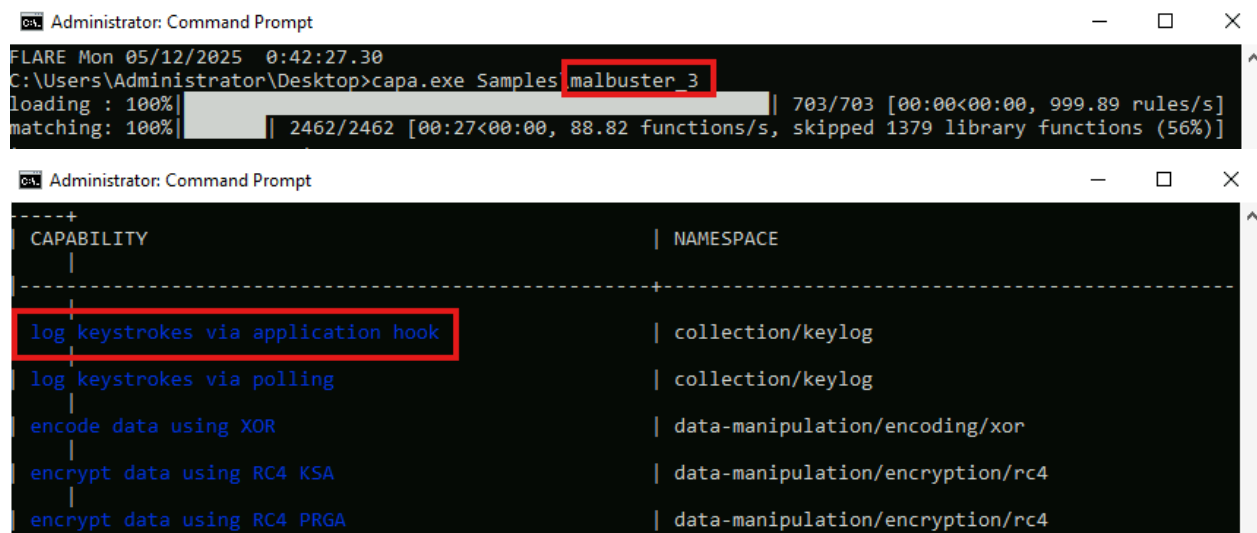
12. Using capa, which binary can log keystrokes?

Igual que la part anterior, utilitzant capa hem hagut de cercar d'un arxiu a un altre quin era el que la capacitat de loggear pulsacions de teclat, com podem observar en aquesta imatge, es mostra que un el malbuster_3 té la capacitat de registrar pulsacions de teclat.

Aquesta funcionalitat és pròpia de keyloggers i suposa un risc greu de filtració de dades.

La comanda:

```
capa.exe Samples\malbuster_3
```



```
Administrator: Command Prompt
FLARE Mon 05/12/2025 0:42:27.30
C:\Users\Administrator\Desktop>capa.exe Samples\malbuster_3
loading : 100%| 703/703 [00:00<00:00, 999.89 rules/s]
matching: 100%| 2462/2462 [00:27<00:00, 88.82 functions/s, skipped 1379 library functions (56%)]
```

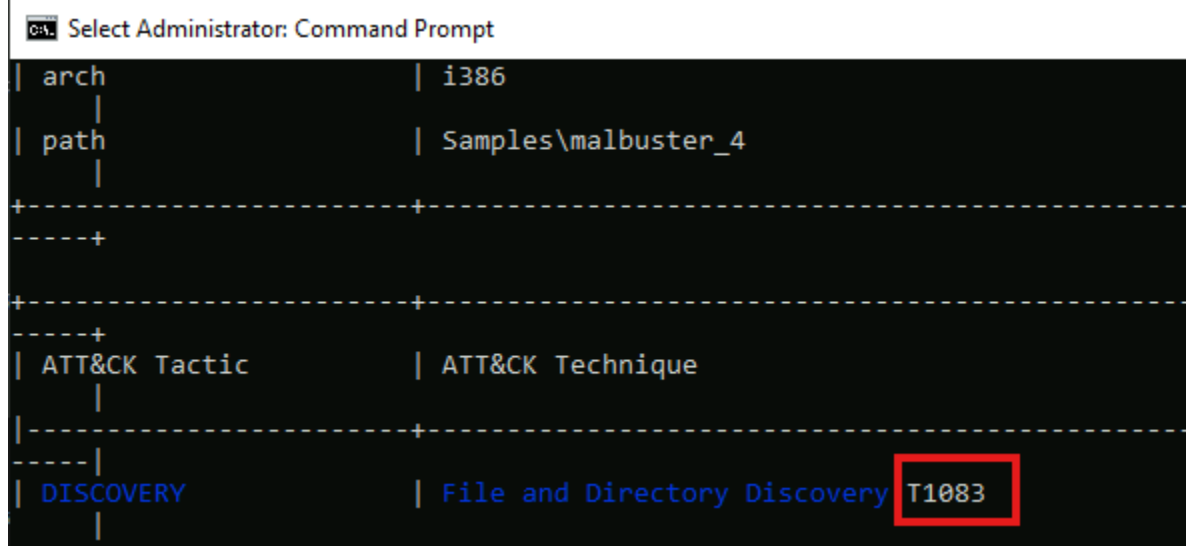
CAPABILITY	NAMESPACE
log keystrokes via application hook	collection/keylog
log keystrokes via polling	collection/keylog
encode data using XOR	data-manipulation/encoding/xor
encrypt data using RC4 KSA	data-manipulation/encryption/rc4
encrypt data using RC4 PRGA	data-manipulation/encryption/rc4

13.What is the MITRE ID of the DISCOVERY technique used by malbuster_4?

Utilitzant CAPA també, hem buscat quin MITRE ID de tècnica de descobriment s'utilitza en malbuster_4. Com podem observar en aquesta captura s'identifica la tècnica T1083. Això permet documentar i entendre millor el comportament de la mostra.

La comanda:

```
capa.exe Samples\malbuster_4
```



arch	i386
path	Samples\malbuster_4
ATT&CK Tactic	ATT&CK Technique
DISCOVERY	File and Directory Discovery T1083

ALERTA! a partir d'ara s'ha utilitzat una màquina Linux!!!

14. Which binary contains the string GodMode?

Des d'una terminal hem cercat els strings de les mostres amb un filtre de cerca perquè només mostres els que continguin el missatge GodMode, una per una fins a trobar quina contenia aquestes strings.

Per fer-ho hem obert el terminal i executat la següent comanda:

ALERTA! en la imatge d'exemple la comanda està sent executada dins de la carpeta on es troba el malware, es troba a **/Desktop/Samples**

```
cd /Desktop/Samples  
string malbuster_x | grep GodMode
```

El que fem és fer un string del malware (Veure tot el contingut del codi) i fer li un grep, el grep es per buscar una paraula específica, en aquest cas es “GodMode”.

Com es pot veure, malbuster_1 lo te la cadena en canvi detecta que malbuster_2 conté la cadena “GodMode”, possiblement associada a funcionalitats ocultes o tècniques d'enginyeria social.

```
ubuntu@ip-10-10-192-162:~/Desktop/Samples$ strings malbuster_1 | grep GodMode  
ubuntu@ip-10-10-192-162:~/Desktop/Samples$ strings malbuster_2 | grep GodMode  
get_GodMode  
set_GodMode  
GodMode
```

15. Which binary contains the string Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)?

Fent el mateix que en l'anterior, però filtrant per Mozilla4.0 em trobat, com es pot observar en la imatge la cadena "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1" en la mostra malbuster_1. Aquesta cadena pot servir per emular trànsit de navegador legítim i evitar deteccions per part de sistemes de seguretat.

Igual que la part anterior amb la comanda:

```
string malbuster_x | grep Mozilla/4.0
```

```
ubuntu@ip-10-10-192-162:~/Desktop/Samples$ strings malbuster_2 | grep Mozilla/4.0
ubuntu@ip-10-10-192-162:~/Desktop/Samples$ strings malbuster_3 | grep Mozilla/4.0
ubuntu@ip-10-10-192-162:~/Desktop/Samples$ strings malbuster_4 | grep Mozilla/4.0
ubuntu@ip-10-10-192-162:~/Desktop/Samples$ strings malbuster_1 | grep Mozilla/4.0
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
ubuntu@ip-10-10-192-162:~/Desktop/Samples$
```

Anàlisi i discussió

L'anàlisi realitzada en aquesta pràctica ens ha permès aprofundir en els mecanismes d'identificació i caracterització de malware mitjançant tècniques d'anàlisi estàtica. S'ha treballat amb quatre mostres diferents de malware (malbuster_1 a malbuster_4), cadascuna amb característiques particulars, i s'han utilitzat eines diverses com pestudio, capa, VirusTotal i abuse.ch per extreure informació rellevant com l'arquitectura, les funcions importades, les signatures de malware i les tècniques MITRE ATT&CK associades.

Hem observat que diverses mostres compartien signatures vinculades a famílies conegudes com a Zeus/Zbot i Razy, indicant comportaments típics de troians bancaris i adware sofisticat. Aquestes deteccions han estat contrastades amb motors d'antivirus com Avira, i a través de metadades i capçaleres PE s'ha pogut deduir informació contextual (com el nom original dels fitxers o les funcions importades des de DLLs crítiques com ShellExecuteA).

Una eina especialment rellevant ha estat capa, que ha permès detectar funcionalitats ocultes com l'ús d'instruccions anti-VM (indicant mecanismes d'evasió), keyloggers (captura de pulsacions) i cadenes relacionades amb l'ofuscació o l'enginyeria social (com "GodMode" o navegadors antics). Això demostra la sofisticació de les binàries analitzades, així com la necessitat d'una avaluació holística per determinar el nivell d'amenaça real.

Conclusions

Aquesta pràctica ha sigut fonamental per comprendre com es poden identificar, analitzar i caracteritzar mostres de malware utilitzant tècniques d'anàlisi estàtica. S'ha pogut comprovar que, mitjançant eines específiques, és possible obtenir molta informació sense executar el binari, cosa que resulta essencial en entorns segurs i controlats com els d'un SOC.

Les mostres analitzades presenten comportaments maliciosos associats a famílies de malware conegudes com Zeus/Zbot i Razy, i s'ha evidenciat l'ús de tècniques avançades d'evasió i persistència. També s'ha pogut detectar funcionalitats orientades a l'espionatge (spyware), manipulació del sistema i fins i tot accions automàtiques en l'obertura dels fitxers.

L'experiència adquirida ens ha permès reforçar la comprensió dels formats PE, les signatures de malware, les eines de detecció i la correlació amb tècniques MITRE. Això representa una base sòlida per a futurs escenaris d'anàlisi dinàmica, resposta a incidents i enginyeria inversa avançada.