Hybrid Analysis 101

Beltrán Rivera Arias

¿Quién soy yo?

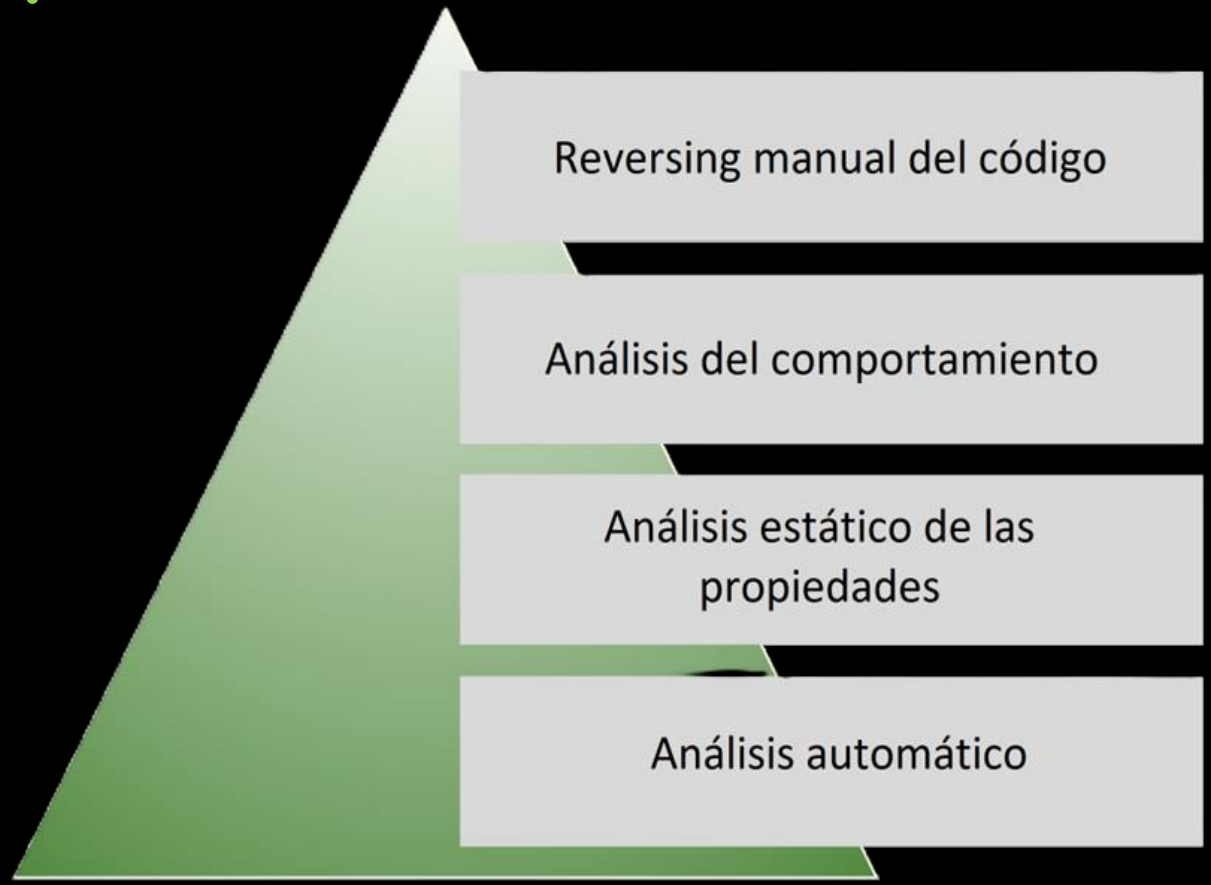
- Security researcher, developer, pentester
- +6 años autodidacta
- All things cyber
- Eterno estudiante del hacking

Índice

- ¿Análisis híbrido?
- Niveles de análisis
- Preanálisis
- Análisis automático
- Análisis estático
- Análisis dinámico
- Obervaciones
- Preguntas

¿Análisis híbrido?

- Preanálisis, automático, estático y dinámico
- Visión completa
- Contextualiza la investigación
- Útil contra antianálisis



Preanálisis

- QCCQ: Qué, Cómo, Cuándo y Quién ha infectado
- Añade contexto importante
- ¿Accidente o ataque?
- Ejecución en entorno aislado

Análisis automático

- Muy rápido
- Variedad de plataformas
- Rápida respuesta
- Poco fiable
- Potencialmente no decisivo

Análisis estático

- Relativamente rápido
- Información más fiable
- Útil contra antidebugging
- Potencialmente decisivo
- Poco útil contra ofuscación
- Requiere experiencia

Análisis dinámico

- Visión más completa
- Muy útil contra ofuscación
- Decisivo
- Largo y tedioso
- Inútil contra antidebugging/antivm

Caso de estudio: Surabaya

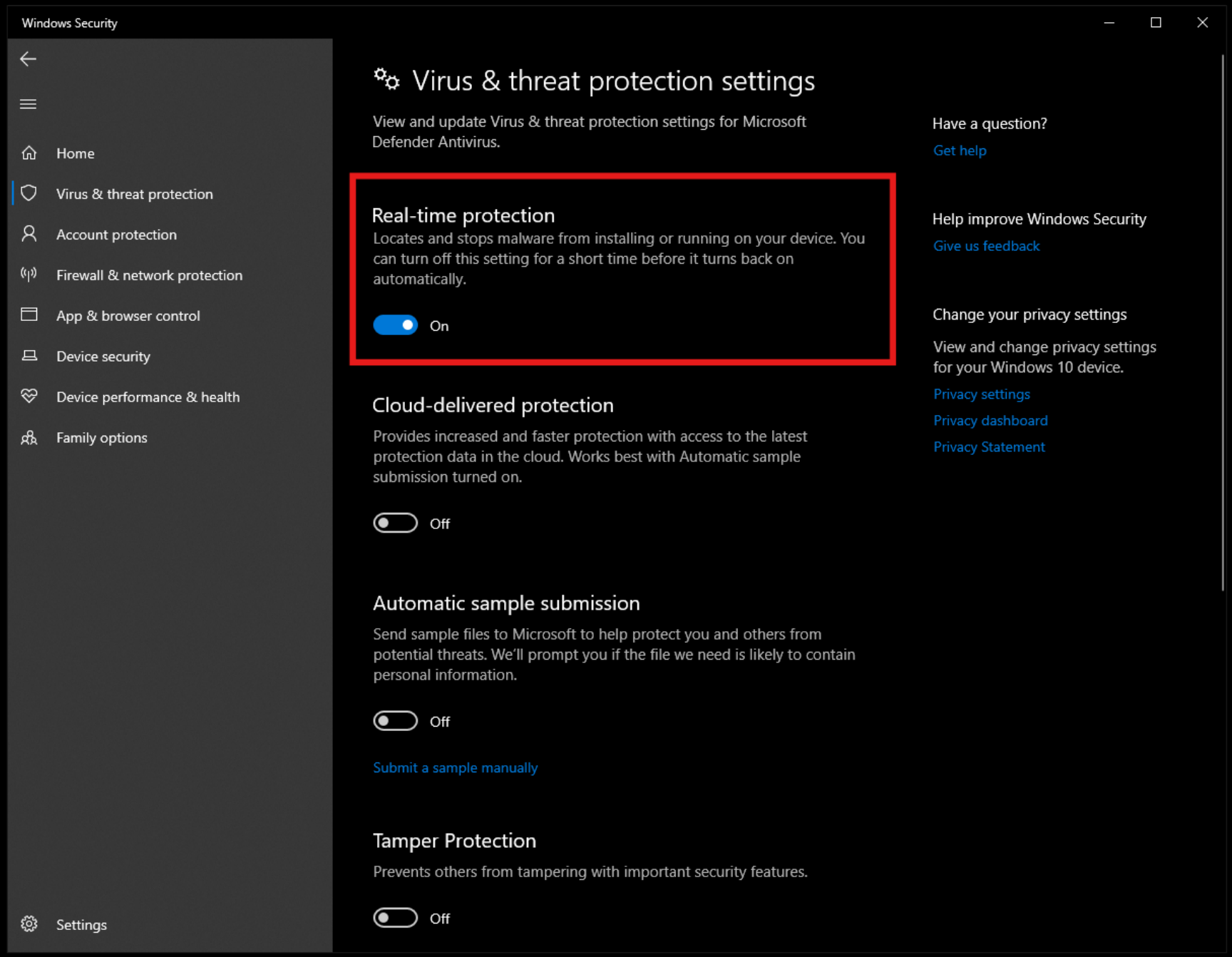
Muestra vieja
Visual Basic 6 (anterior a .NET)
Ausencia de disassemblers/decompilers
Codename: Worm:Win32/SillyShareCopy.E
Formato: ISO

Preanálisis

Laboratorio

WINDOWS 10

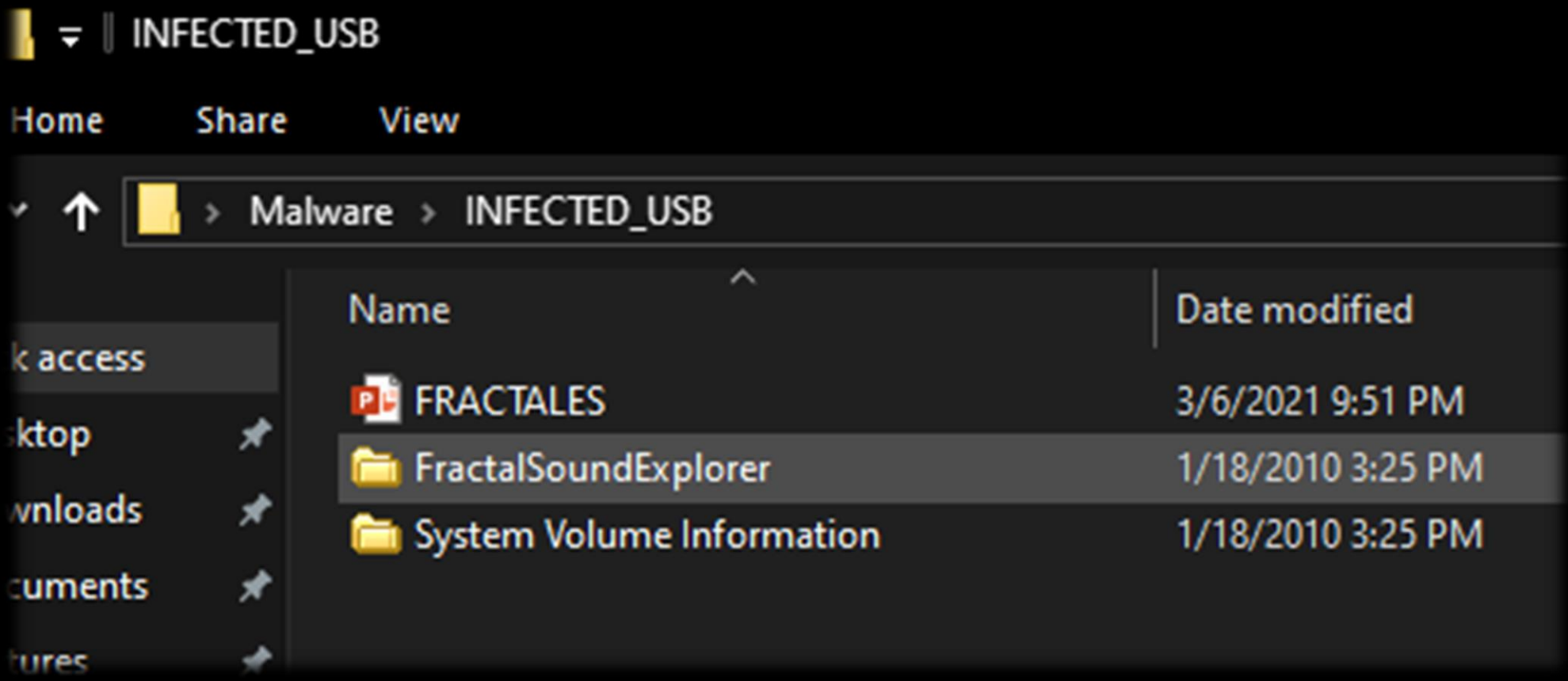
INSTALAR
HERRAMIENTAS


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Virus & threat protection settings
View and update Virus & threat protection settings for Microsoft Defender Antivirus.
Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.
On
Cloud-delivered protection
Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.
Off
Automatic sample submission
Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.
Off
Submit a sample manually
Tamper Protection
Prevents others from tampering with important security features.
Off
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

Primera ejecución

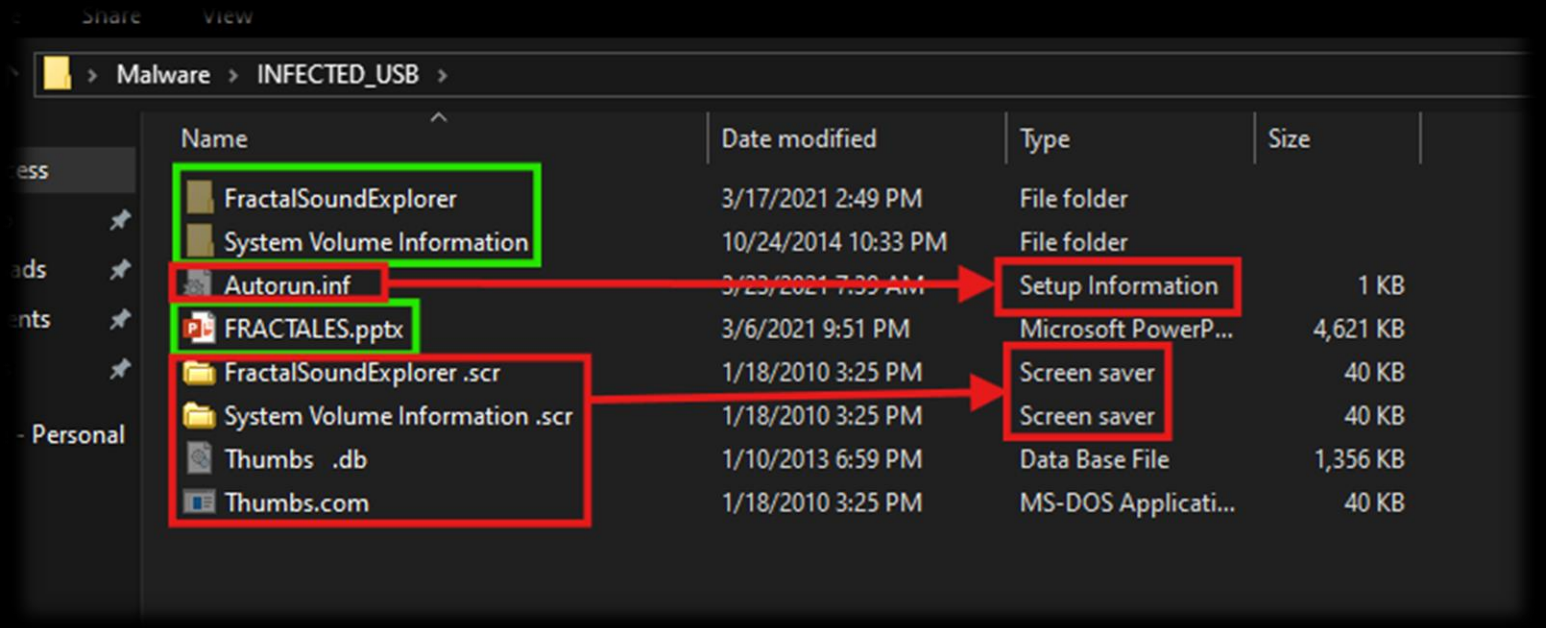
- Detección a simple vista
- Fácil
- Ayuda con los siguientes pasos
- Configurar la MV lo mínimo

La cara

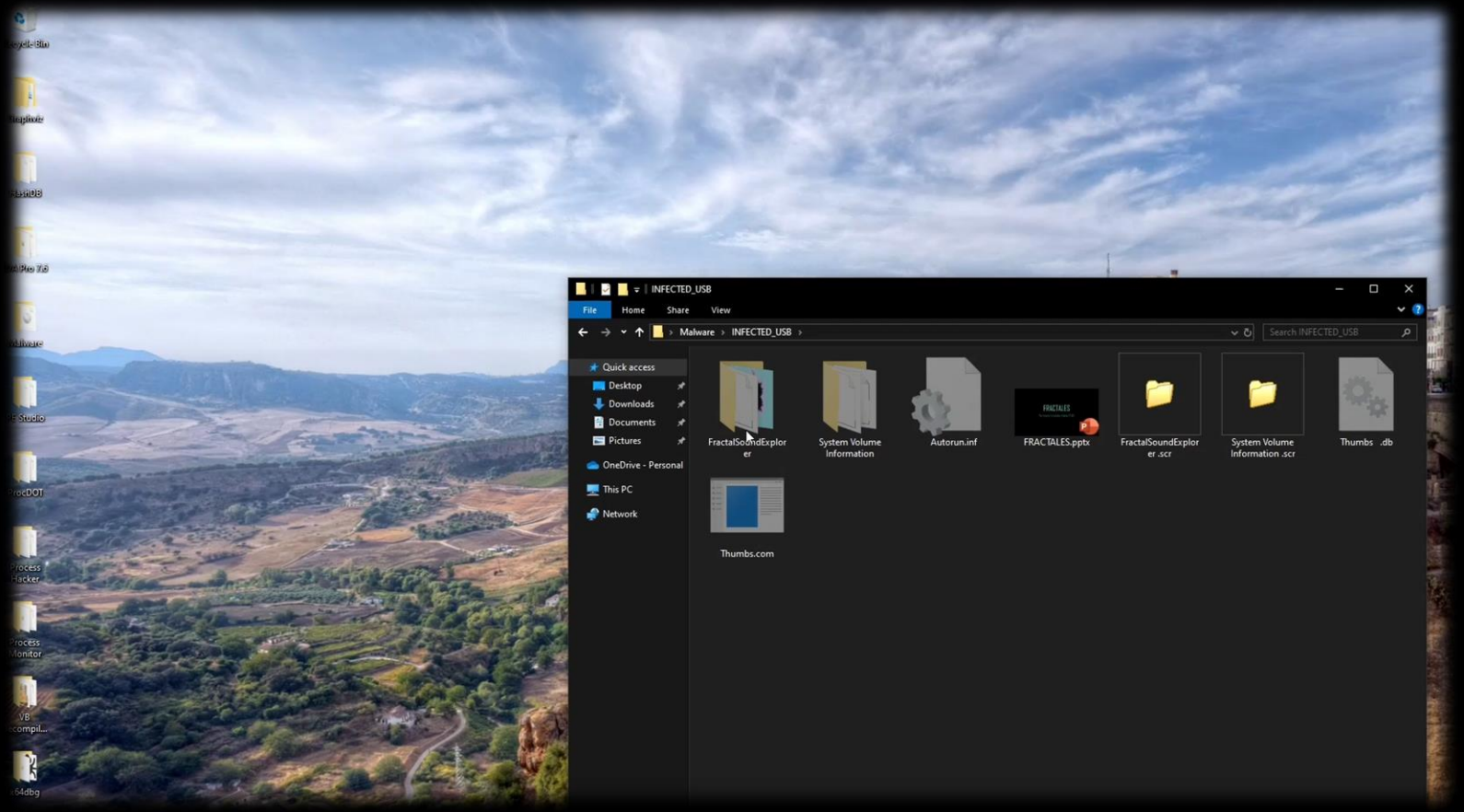

INFECTED_USB
Home
Share
View
Malware
INFECTED_USB
Name
Date modified
FRACTALES
3/6/2021 9:51 PM
FractalSoundExplorer
1/18/2010 3:25 PM
System Volume Information
1/18/2010 3:25 PM

La cruz

- ¿Carpetas duplicadas?
- ¿Salvapantallas con iconos de carpeta?
- ¿Ejecutable para MS-DOS?



Ejecución


INFECTED_USB
File
Home
Share
View
Malware
INFECTED_USB
Search INFECTED_USB
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive - Personal
This PC
Network
FractalSoundExplorer
System Volume Information
Autorun.inf
FRACTALES.pptx
FractalSoundExplorer.scr
System Volume Information.scr
Thumbs .db
Thumbs.com

Suplanta carpetas

Suelta archivos

¿Qué sabemos?

Se ejecuta en segundo plano

Es malicioso

¿Qué **no** sabemos?

- ¿Cómo lo hace?
- ¿Hace algo más que no sepamos?
- ¿Establece persistencia?
- ¿Roba datos?
- Etcétera

Análisis automático

Objetivos del análisis automático

- Determinar detalles técnicos
- Obtener una segunda impresión
- Ante la duda, seguir con el análisis

Plataformas

VirusTotal

Público

Fácil de usar

Sandboxes

Fiable, pero no decisivo

No soporta varios archivos

AnyRun

Más avanzado

Interactivo

Configurable

Potencialmente decisivo

Soporta varios archivos*

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE | URL | SEARCH

Choose file

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

66 / 72

Community Score -105

66/72 security vendors flagged this file as malicious

Reanalyze | Similar | More

97bfa55df8d6d8f94da54feb832ce5f7c27e934dacad6fb31f8fe92c1206b61b

FractalSoundExplorer .scr

peexe | idle | usb-autorun

Size 40.00 KB

Last Analysis Date 2 months ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 8

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

Popular threat label worm.bant/sillyshare

Threat categories worm | trojan

Family labels bant | sillyshare | sillysharecopy

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Worm/Win32.AutoRun.R2381	Alibaba	Worm:Win32/vobfus.1030
AliCloud	Worm:Win/SillyShareCopy.Gen	ALYac	Trojan.VB.NKU
Antiy-AVL	Worm/Win32.AutoRun	Arcabit	Trojan.VB.NKU
Arctic Wolf	Unsafe	Avast	Win32:VB-EIK
AVG	Win32:VB-EIK	Avira (no cloud)	TR/VB.aei
Baidu	Win32.Trojan.VB.iy	BitDefender	Trojan.VB.NKU
Bkav Pro	W32.QuvroBjngL.Trojan	ClamAV	Win.Worm.VB-632

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 8

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

Basic properties

MD5	20f1b63d80aca45206aedf66fe20a5aa
SHA-1	199b28914d4e95e165885fdce605f3d58f47e42f
SHA-256	97bfa55df8d6d8f94da54feb832ce5f7c27e934dacad6fb31f8fe92c1206b61b
Vhash	0440361d0f1"z
Authentihash	d1d294cc5356dce209002e83c1e0e6b4ac2bb79510d75b32c23f35d50b6a79bc
Imphash	b52df0bbf59016bbef9115e588a0c6bd
Rich PE header hash	9fd14c40d4dca5e21aa54c626075766f
SSDEEP	384:CXWT1aHFF0yoltTrpsYbZWwBYmax1433EAE7tS+yvtzle/tfF17e/7e/KCe/+P:cWTkFFHbgtmaxmkAEBSLvL5nC6m
TLSH	T1F603C402779351B6EBBB557909A1C24682B77C394F274D4B33452D7E3D30E922D2AB13
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win64 Executable (generic) (37.3%) | Win16 NE executable (generic) (17.8%) | Win32 Executable (generic) (15.9%) | Windows Icons Library (generic) (7.3%) | OS/2 Exec…
DetectItEasy	PE32 | Linker: Microsoft Linker (6.0)
Magika	PEBIN
File size	40.00 KB (40960 bytes)
PEiD packer	Microsoft Visual Basic v5.0/v6.0

History

Creation Time	2007-01-28 04:00:37 UTC
First Submission	2008-03-28 18:19:35 UTC
Last Submission	2025-03-03 19:34:18 UTC
Last Analysis	2025-03-03 19:34:30 UTC

Names

FractalSoundExplorer .scr
System Volume Information .scr
Thumbs.com
$Recycle.Bin .scr
20f1b63d80aca45206aedf66fe20a5aa.vir
Adobe Online.com
$AVG .scr
09 .scr
aa
SYYmMAqRz.caj

Portable Executable Info

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 8

Contacted Domains (2)

Domain	Detections	Created	Registrar
res.public.onecdn.static.microsoft	0 / 94	2023-05-05	MarkMonitor Inc.
vboxsvr.ovh.net	5 / 94	1998-06-08	OVH sas

Contacted IP addresses (9)

IP	Detections	Autonomous System	Country
104.98.118.146	0 / 94	20940	US
104.98.118.163	0 / 94	20940	US
192.168.0.51	0 / 94	-	-
20.69.140.28	0 / 94	8075	US
20.99.133.109	0 / 94	8075	US
20.99.186.246	0 / 94	8075	US
23.213.37.172	0 / 94	16625	US
23.221.103.220	0 / 94	16625	US
23.32.75.39	0 / 94	20940	US

Execution Parents (1)

Scanned	Detections	Type	Name
2025-03-06	56 / 68	ZIP	AYANTE_USB.zip

66 / 72

Community Score -105

66/72 security vendors flagged this file as malicious

Reanalyze | Similar | More

97bfa55df8d6d8f94da54feb832ce5f7c27e934dacad6fb31f8fe92c1206b61b

FractalSoundExplorer .scr

peexe | idle | usb-autorun

Size 40.00 KB

Last Analysis Date 2 months ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 8

Display grouped sandbox reports

CAPE Sandbox	0	1	0	0	0	0	Microsoft Sysinternals	0	0	0	0	0	11
Tencent HABO	0	0	0	0	0	0	VirusTotal Cuckoofork	0	0	0	0	0	2
Yomi Hunter	0	0	0	0	0	0	Zenbox	0	2	0	0	0	0

Activity Summary

Download Artifacts | Full Reports | Help

Detections
NOT FOUND

Mitre Signatures
1 HIGH | 1 INFO

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
NOT FOUND

Network comms
2 DNS | 11 IP

Behavior Tags

idle

MITRE ATT&CK Tactics and Techniques

— Defense Evasion TA0005

Masquerading T1036

Severity	Description	Match
HIGH	Icon mismatch, binary includes an Icon from a different legit application in order to fool users	-

— Discovery TA0007

System Information Discovery T1082

Severity	Description	Match
INFO	Reads software policies	-

— Command and Control TA0011

Application Layer Protocol T1071

Severity	Description	Match
UNKNOWN	Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.	-

File system actions

Files Opened

- C:\WINDOWS\system32\imm32.dll
- C:\WINDOWS\system32\lpk.dll
- C:\WINDOWS\system32\psapi.dll
- C:\WINDOWS\system32\usp10.dll
- C:\WINDOWS\system32\winime32.dll
- C:\WINDOWS\system32\ws2_32.dll
- C:\WINDOWS\system32\ws2help.dll
- C:\Users\user\Desktop\program.exe
- C:\Windows\AppPatch\sysmain.sdb
- C:\Windows\SysWOW64\KERNEL32.DLL

Files Deleted

- C:\Windows\System32\wbem\Performance\WmiApRpl.h
- C:\Windows\System32\wbem\Performance\WmiApRpl.ini

Registry actions

Registry Keys Opened

- \REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
- \REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
- \Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
- \Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
- \Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MUI\UILanguages\en-US
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap

Process and service actions

Processes Created

- %SAMPLEPATH%\97bfa55df8d6d8f94da54feb832ce5f7c27e934dacad6fb31f8fe92c1206b61b.exe
- C:\Users\user\AppData\Local\Temp\ea08d4a10990d91ee465cfa3c270e3a6.exe
- C:\Windows\system32\wbem\wmiprvse.exe -Embedding
- \??\C:\Windows\system32\conhost.exe -1047381220-1025366142-2600100401104419999118291342214609926921760871039-718809777
- \??\C:\Windows\system32\conhost.exe -1361093184-996115534-591420690-1163420689-175319401710363787362436245319569217 11
- \??\C:\Windows\system32\conhost.exe -1377075561-203863304116070622 38-2056268955136294707 6-16622522391590774337-1602150964
- \??\C:\Windows\system32\conhost.exe -1433651241-432189305427563205639060018-180476341413975591762976022 88-1883496784
- \??\C:\Windows\system32\conhost.exe -156869107415401928351746869632-1798706562-1903389835157296089 5-1754845428-1355110895
- \??\C:\Windows\system32\conhost.exe -1743272765-655294516465288594-608636042-339993225-159327858603278525-1772865788
- \??\C:\Windows\system32\conhost.exe -1749178045963408539167168659 1-1783269839-821822246-16369388812144973389679128079

Nueva información

- Claves de registro
- Archivos
- Comandos
- Árbol de procesos

Nuevos desafíos

- Asumimos falsos positivos y negativos
- Demasiado ruido
- Desconocemos el flujo de ejecución
- Desconocemos parte de las TTPs

Análisis estático

Objetivos generales

ENCONTRAR IOCS

CONOCER TECNOLOGÍAS USADAS

DETERMINAR TÁCTICAS ANTIANÁLISIS

RECABAR DETALLES TÉCNICOS

Determinar librerías

- Habituales
- Poco habituales
- Desconocidas
- ¿Se usan habitualmente con fines maliciosos?

Determinar etapas posteriores de despliegue

- Código ofuscado
- Recursos empaquetados/comprimidos
- Recursos encriptados
- Otros recursos

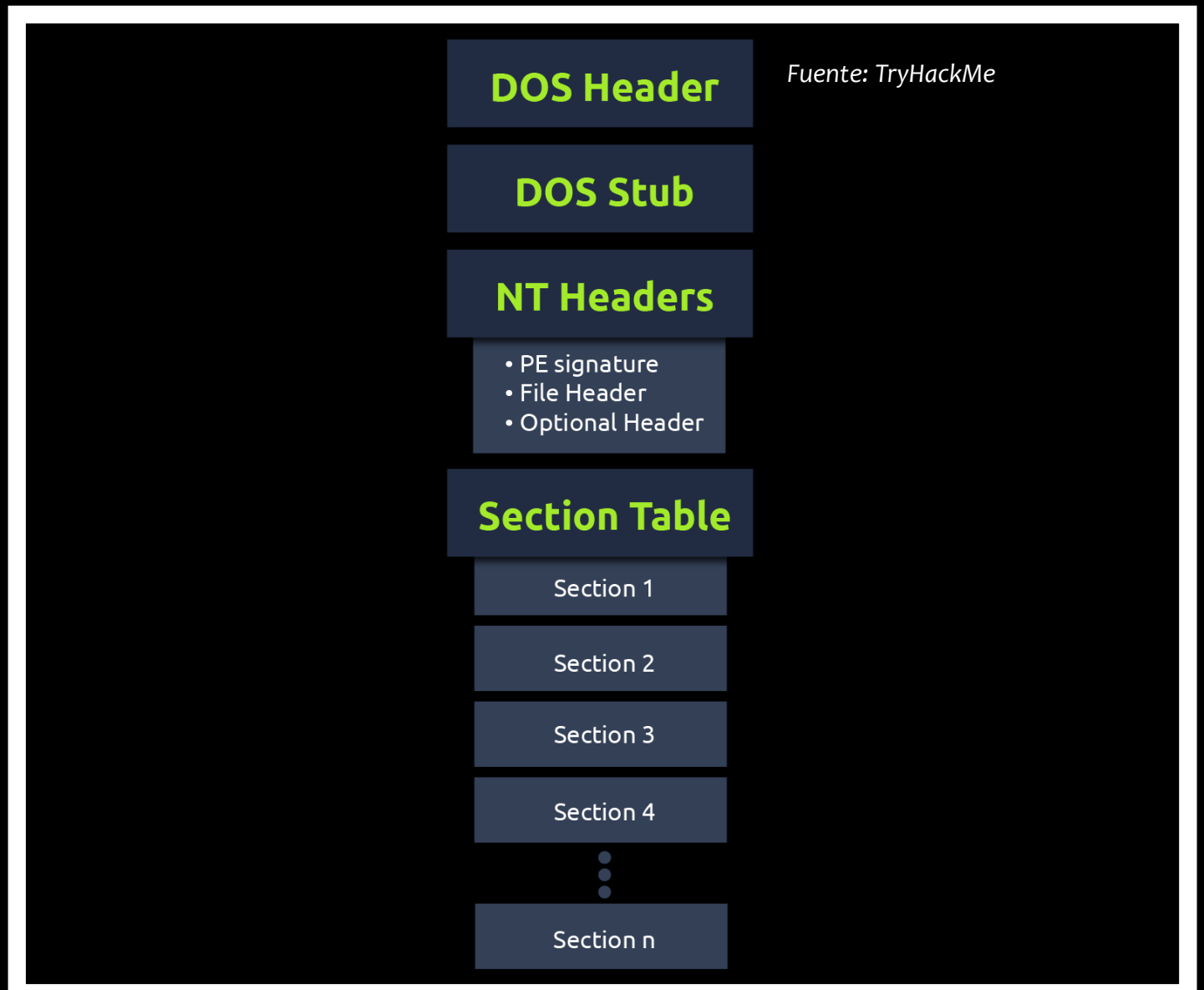
Objetivos concretos

Funciones a cazar

- Funciones conocidas
  - **ShellExecute/ShellExecuteEx** – Ejecuta comandos
  - **CreateRemoteThread** – Usado para inyectar código
  - **VirtualAllocEx** – Usado para inyectar código
  - **ReadProcessMemory/WriteProcessMemory** – Usado para inyectar código
- Funciones… ¿desconocidas?
  - MS Docs
  - Internet
    - Google
    - Si Google falla → Yandex

Herramientas

- Software
  - PE Studio
  - Detect it Easy (DiE)
  - 7zip
- Máquinas Virtuales
  - Ubuntu/Kali/Otro Linux
  - Windows



Fuente: TryHackMe

¿Qué es un PE?

Secciones

¿Qué son las secciones en un ejecutable?

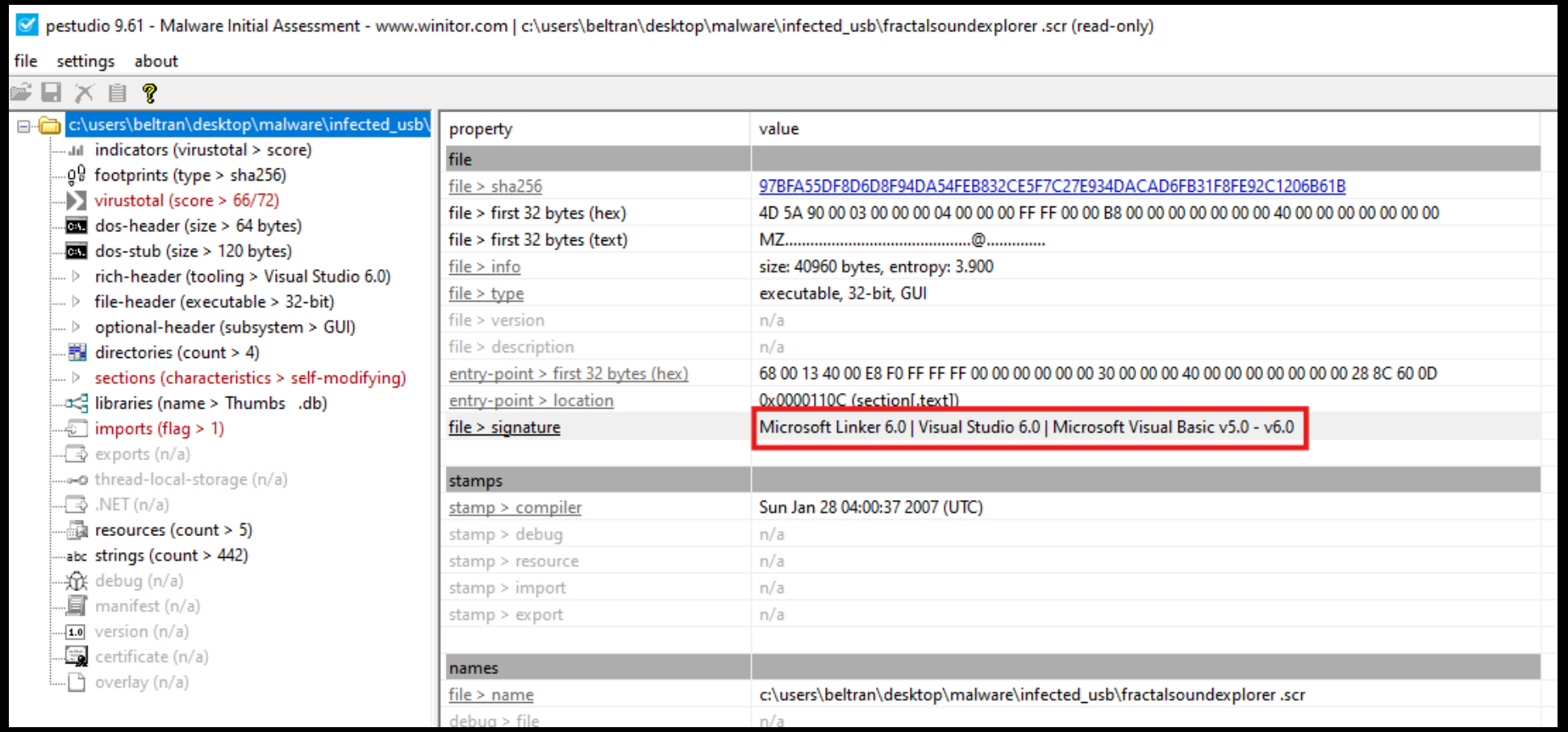
Algunas secciones habituales:

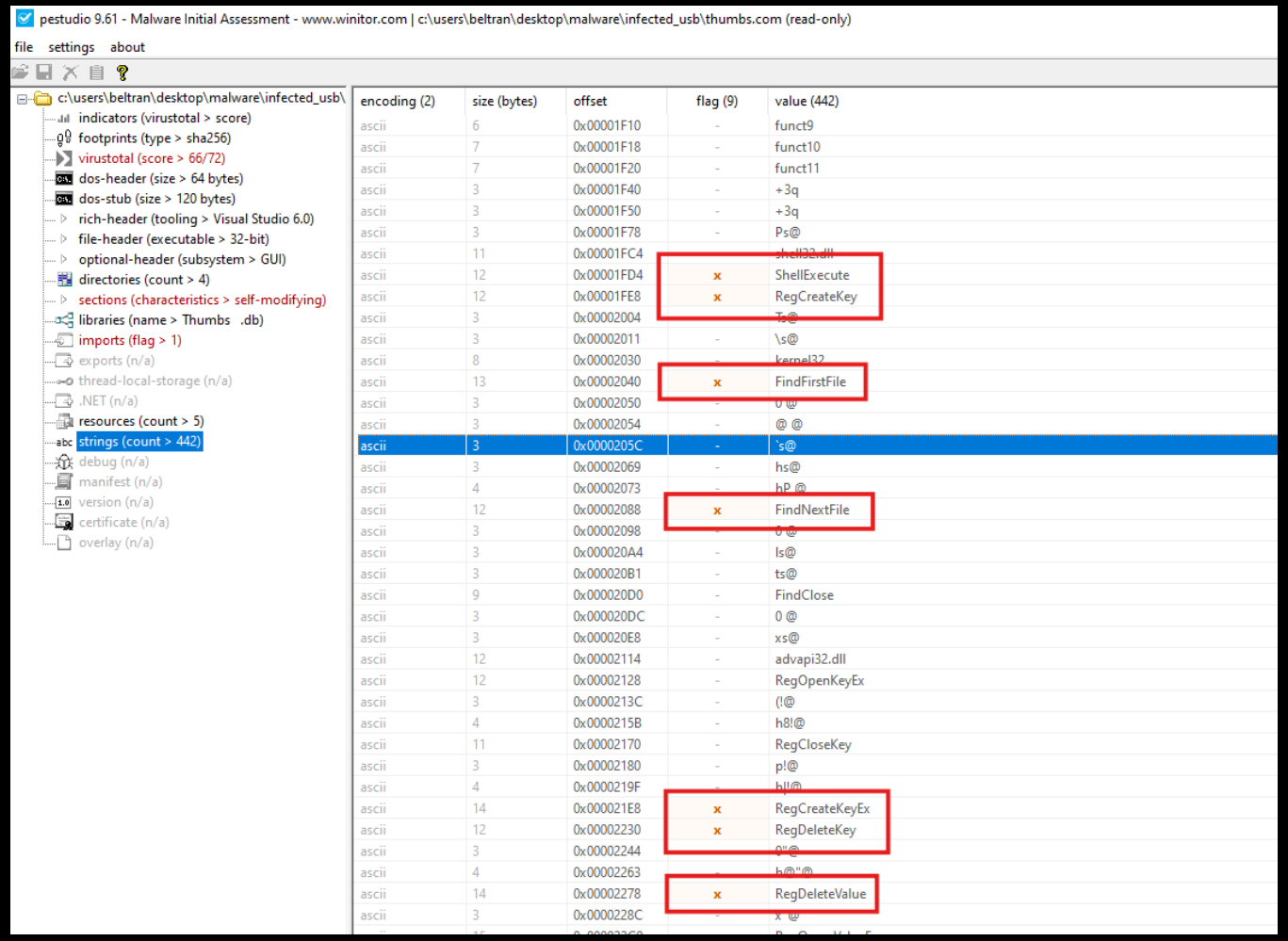
- .text – Código
- .data – Datos inicializados (variables) – ***int myNum = 6;***
- .bss – Datos sin inicializar (variables) – ***int myNum;***
- .rdata – Datos inicializados (constantes) – ***const int myNum = 6;***
- .rsrc – Recursos (imágenes, audio, otros archivos)

PEStudio

- Información del ejecutable
- Texto
- Dependencias
- Funciones importadas
- Funciones exportadas
- IOCs

Información del ejecutable

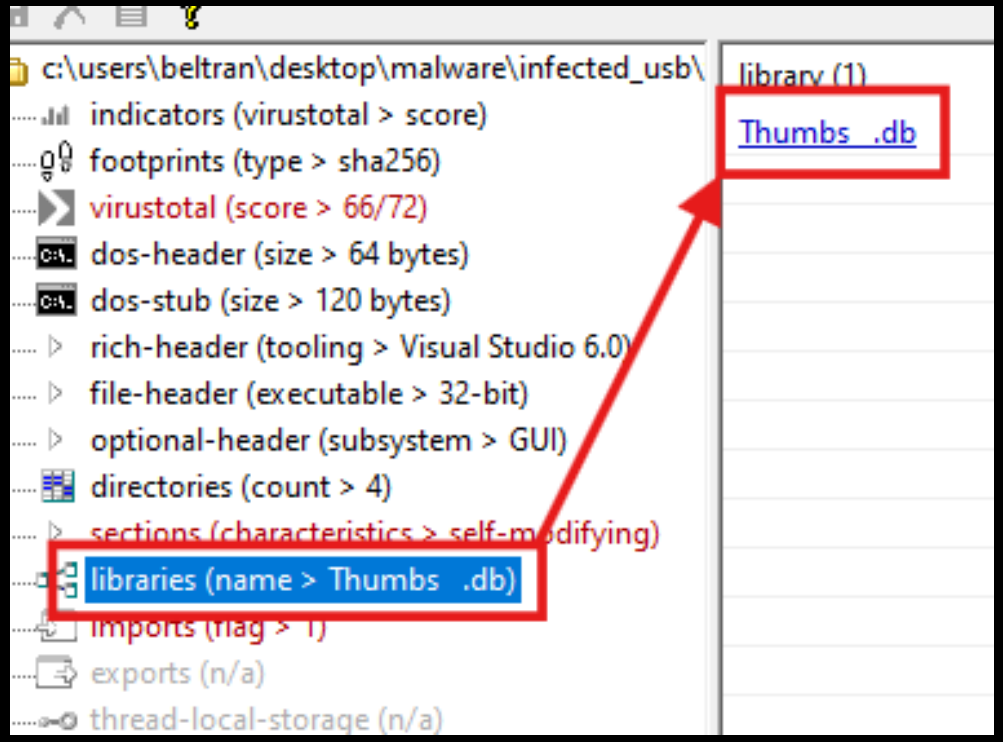


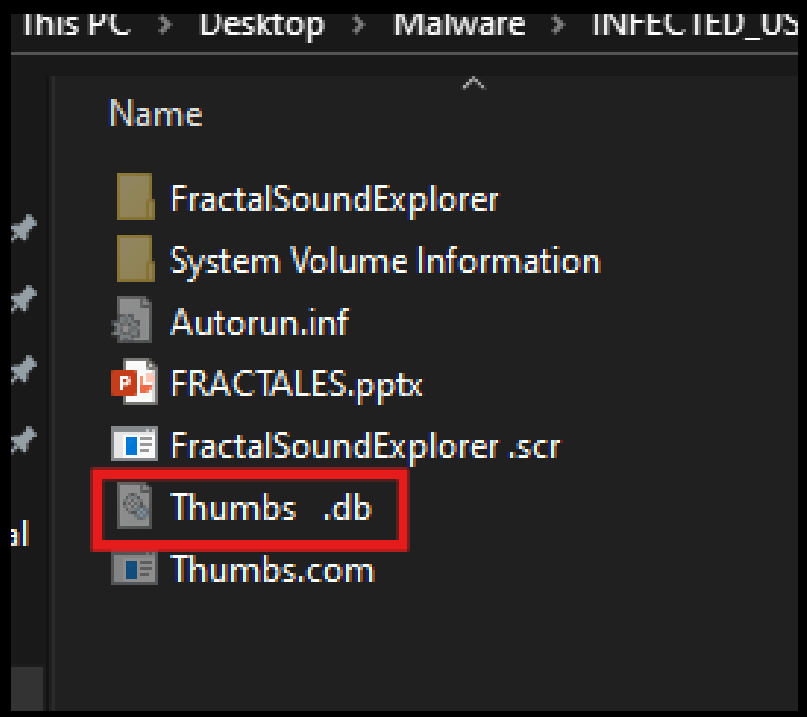


Strings

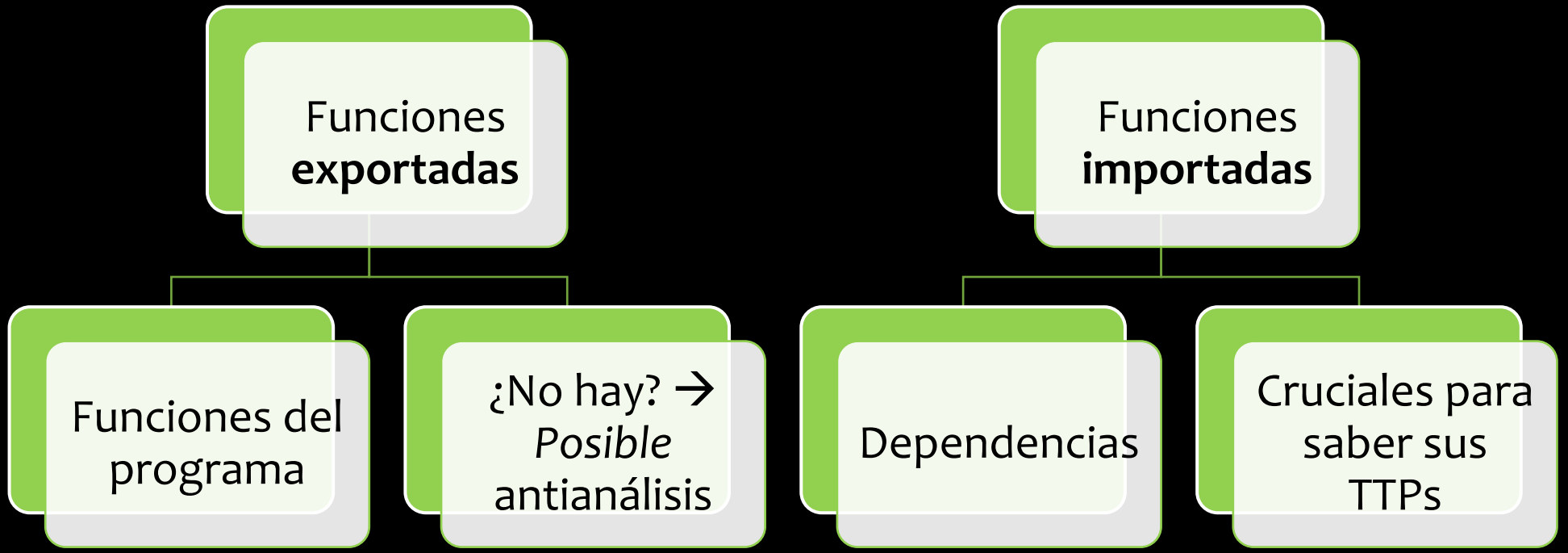
- Importaciones ocultas
- Scripts
- Pistas

Dependencias



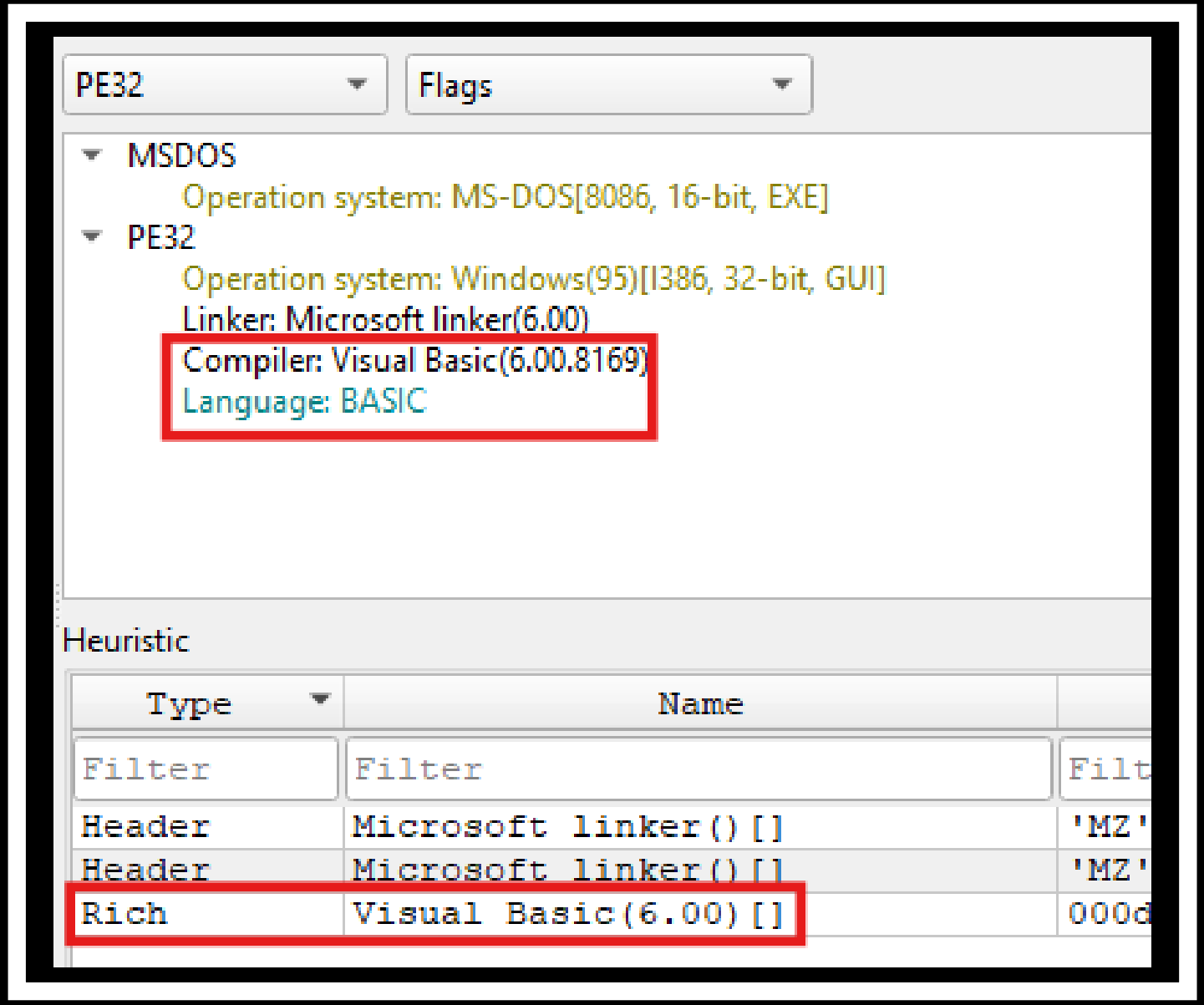


Funciones


Funciones **exportadas**
Funciones del programa
¿No hay? → *Posible* antianálisis
Funciones **importadas**
Dependencias
Cruciales para saber sus TTPs

DiE

- Entropía
  - Detección de compresión/encriptación
- Detección de compilador y lenguaje
- Detección de archivos embebidos

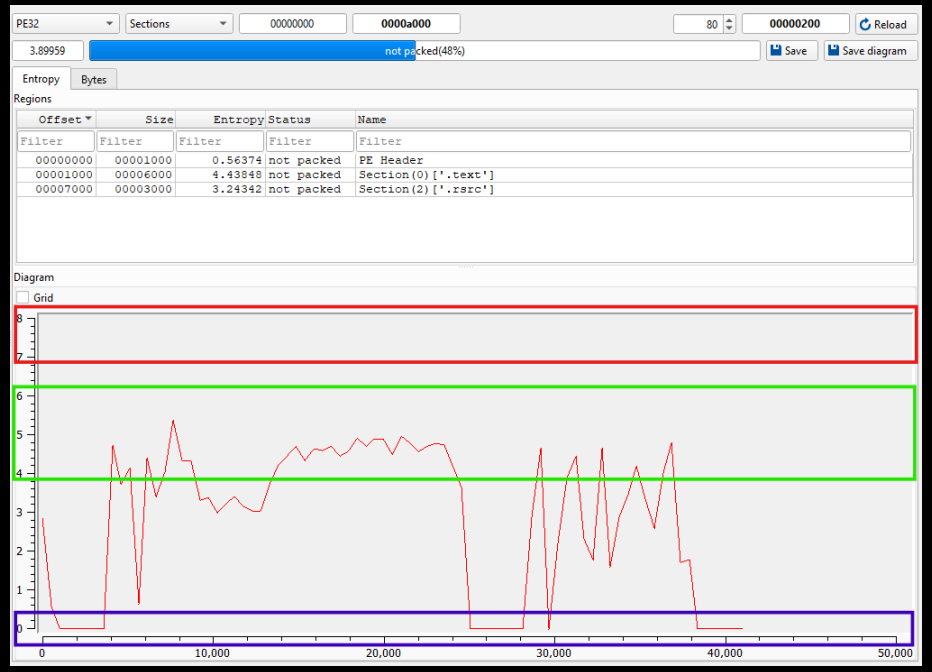


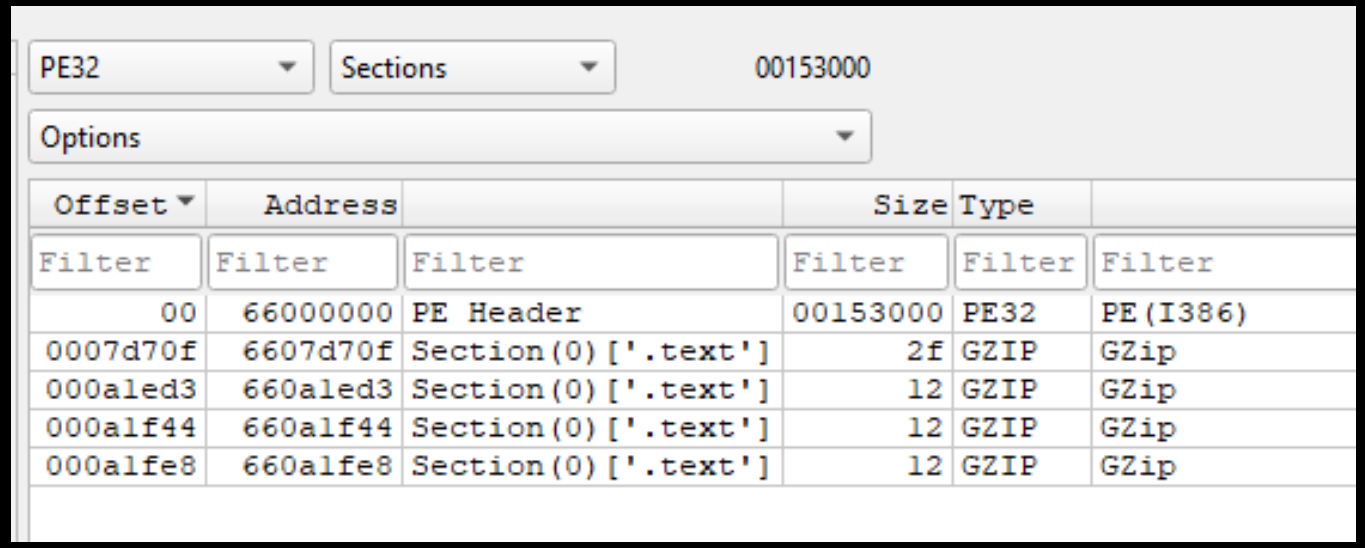
Compilador y lenguaje

- Útil para reversing posterior
- Resuelve posibles dudas técnicas

Entropía, compresión y encriptación

- **¿Qué es?**
  - Medida del desorden
  - Detecta compresión/encriptación
- **¿Cómo se usa?**
  - Rojo (7-8): Compresión/encriptación
  - Verde (4-6): Texto
  - Azul (0): Padding





Extracción de archivos

- Detecta archivos embebidos
- Etapas secundarias
- Utilidades del malware
- Otros archivos maliciosos

Nuevos datos

- ¿Hay más stages/etapas?
- Funciones habituales
- Otros recursos

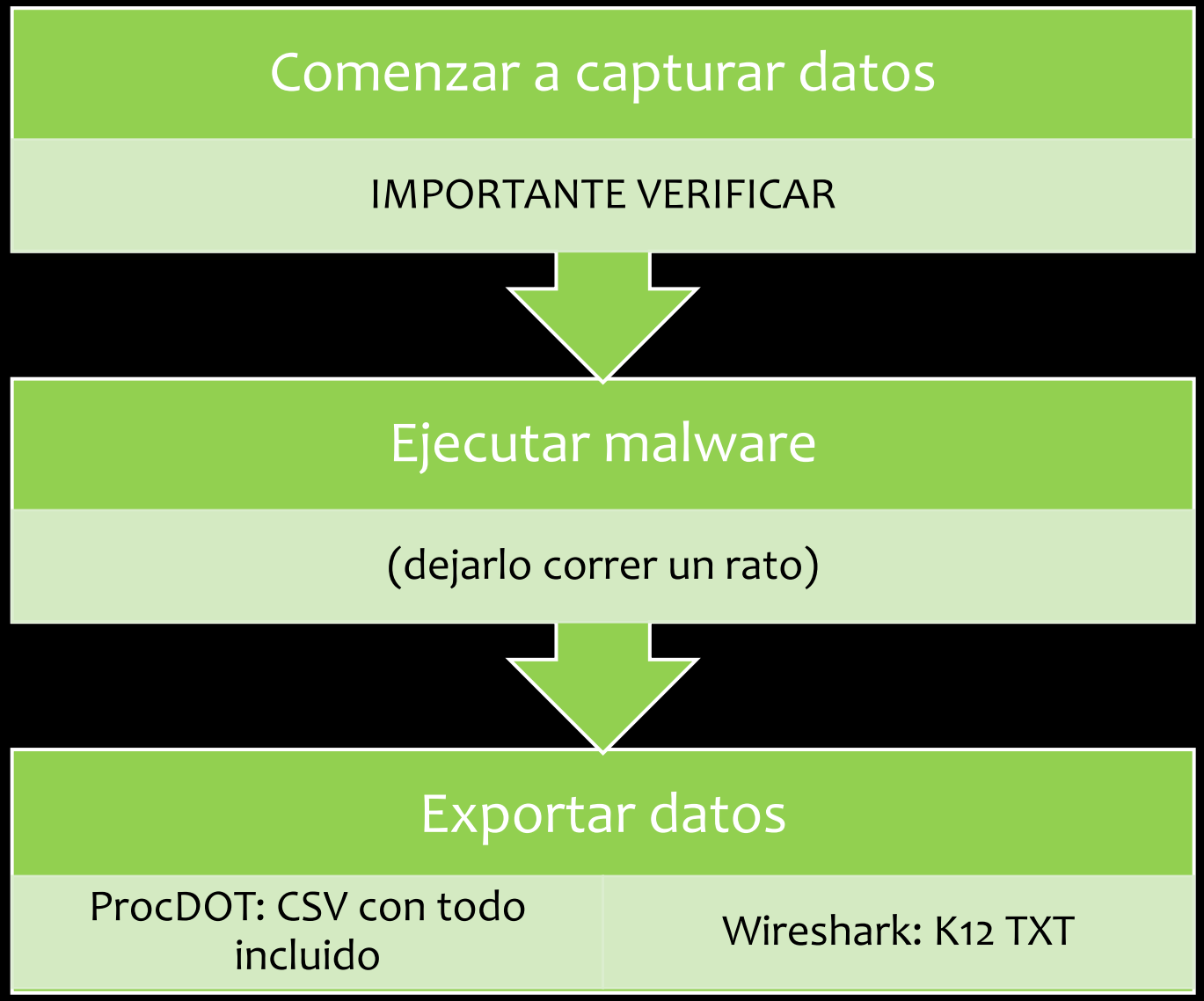
Análisis dinámico

Objetivos

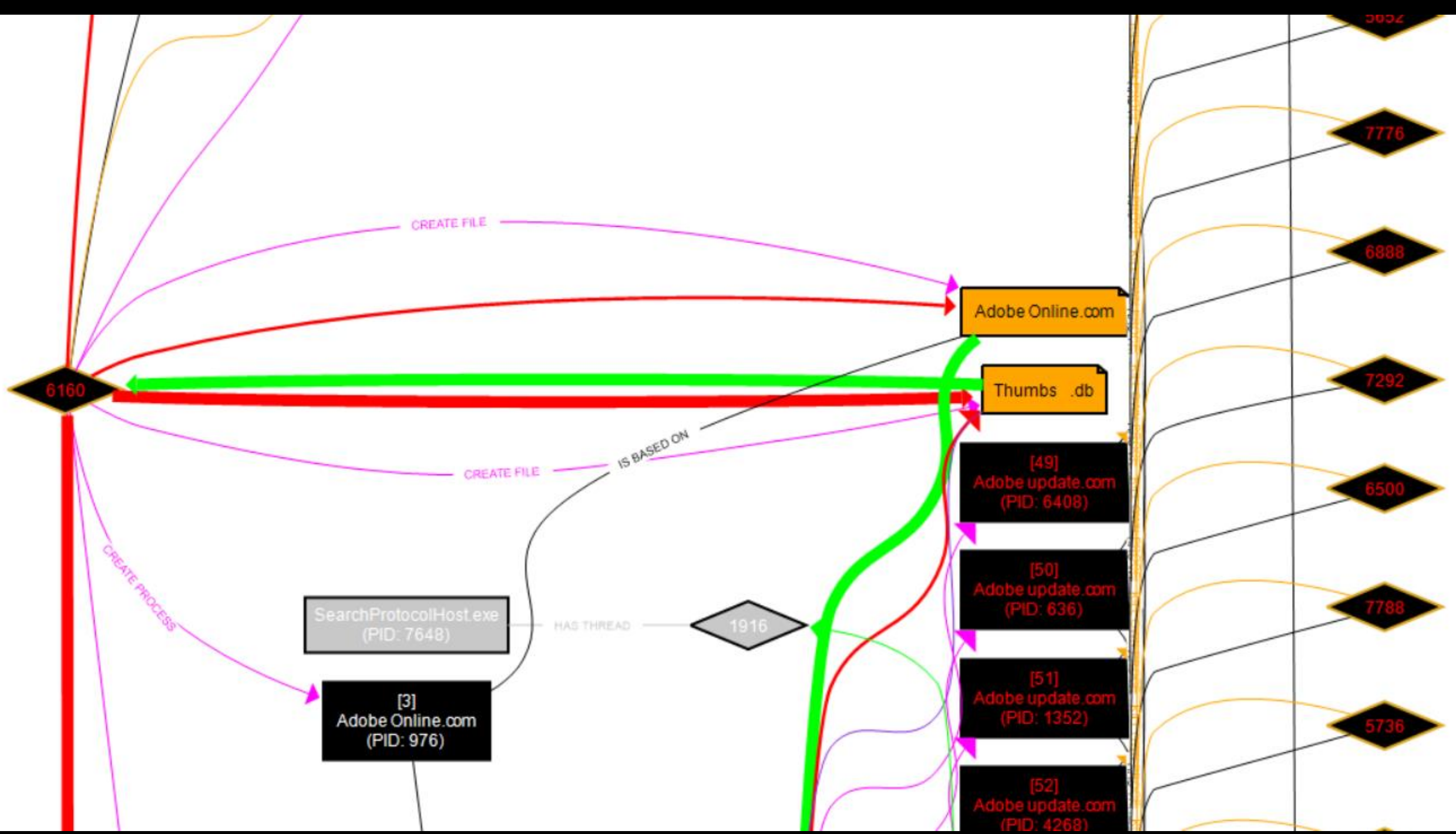
- Comportamiento
- Registro/archivos precisos
- ¿Artefactos?
- ¿C2?

Herramientas

- ProcDOT
- Graphviz
- Windump
- Wireshark
- ProcMon (SysInternals)


Comenzar a capturar datos
IMPORTANTE VERIFICAR
Ejecutar malware
(dejarlo correr un rato)
Exportar datos
ProcDOT: CSV con todo incluido
Wireshark: K12 TXT

Detonación


CREATE FILE
Adobe Online.com
6160
Thumbs .db
CREATE FILE
IS BASED ON
[49]
Adobe update.com
(PID: 6408)
CREATE PROCESS
SearchProtocolHost.exe
(PID: 7648)
HAS THREAD
1916
[50]
Adobe update.com
(PID: 636)
[3]
Adobe Online.com
(PID: 976)
[51]
Adobe update.com
(PID: 1352)
[52]
Adobe update.com
(PID: 4268)
5652
7776
6888
7292
6500
7788
5736

Observaciones

¿Por qué importa ahora el análisis estático junto al dinámico?

- ¿Qué y cómo?
- ¿Nos hemos perdido algo?
- Análisis informado

Redacción de informe

- Obsidian/Visio/draw.io (gráficos)
- Obsidian/Word (redacción)

Detalles técnicos y TTPs

- ¿Cómo es el acceso inicial?
- ¿Persiste? ¿Cómo?
- ¿Se propaga? ¿Cómo?
- ¿Exfiltra datos? ¿Cuáles?
- ¿Alguna cosa más?

Mitigación y respuesta

- ¿Cómo se elimina?
- ¿Cómo se previene?
- ¿Pasos posteriores de respuesta?

¿Preguntas?