

# Panda Security

Introducción al análisis de malware.



[pandasecurity.com](https://www.pandasecurity.com)

---

# Get-NetNeighbor

- Ximo Molina López
- [t.me/expetec](https://t.me/expetec)
  
- Yassin Said Esteller
- [t.me/saiestyas](https://t.me/saiestyas)
  
- Formamos parte del equipo de PandaLabs como técnicos de Adaptive Defense.



# Panda Security

1. Introducción.
2. Laboratorio de análisis.
3. Introducción al análisis estático.
4. Introducción al análisis dinámico.
5. Ejercicios prácticos.

---

# Introducción

## ¿Porqué aprender reversing?

El objetivo de la ingeniería inversa es obtener información acerca de un producto, para ello se determinan los diferentes elementos que lo componen, como estos interactúan y como fueron desarrollados.

En el ámbito del software la ingeniería inversa nos ayuda a comprender como funciona un programa o aplicación.

De este modo, podemos ver como un elemento afecta a nuestro sistema o incluso entender como llega a realizar ciertas tareas.

---

# Introducción

## ¿Porqué aprender reversing?

La seguridad informática es el área de la informática y telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ella.

Realizar tareas de ingeniería inversa nos brinda información muy útil como:

- Vectores de entrada. ¿Por qué canal ha llegado el malware?
- Indicadores de compromiso. ¿Qué hace sobre nuestro sistema?
- Tareas de mitigación o prevención. ¿Qué vulnerabilidades explota? ¿Podemos remediarlo?
- Impacto sobre la compañía. ¿Hubo fuga de datos?

---

# Introducción

## Tipos de amenazas

Podemos encontrar multitud de clasificaciones y maneras de definir al malware, esta es una de las más comunes:

- Minner: Obtiene recursos de la máquina para realizar minado de criptomonedas.
- Information stealer: Su objetivo es extraer información de un sistema para luego retransmitirlo al atacante.
- Backdoor: Código malicioso que se auto-instala con el fin de brindar acceso al atacante.
- Botnet: Similar al backdoor, solo que en este caso existe una red de máquinas esperando recibir ordenes desde un command and control.
- Downloader: Se encarga de descargar más contenido malicioso.
- Rootkit: Diseñado para ocultar su presencia y ejecutarse con privilegios de administrador.
- Ransomware, cifra ficheros y exige el pago de un rescate para eliminar la amenaza.

---

# Introducción al análisis estático

## Laboratorio de análisis – Primeros pasos

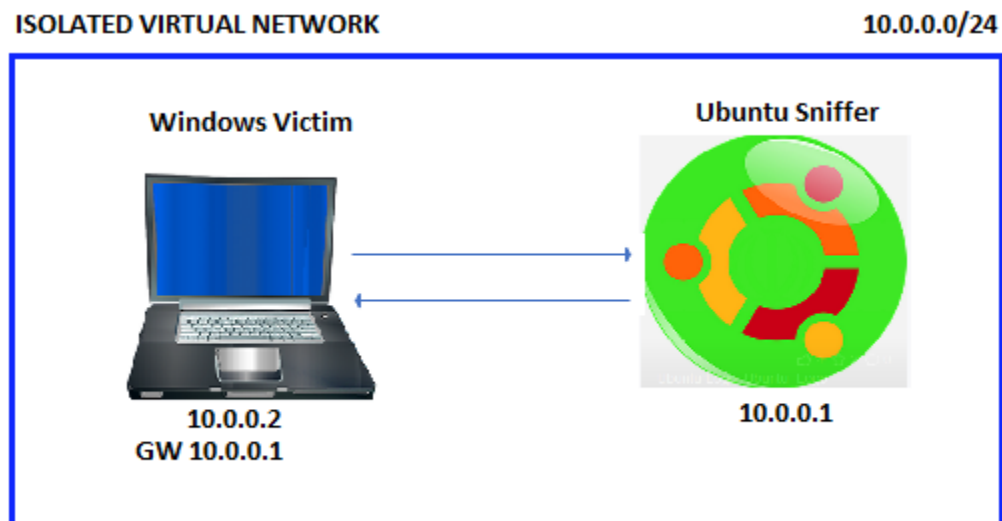
Para ello las herramientas que serán necesarias son:

- VirtualBox
- Una imagen de Windows, descargable de forma gratuita desde <https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>
- Internet Simulation Suite (InetSim)
- Una máquina complementaria, cualquier distribución de linux, para realizar tareas de sniffer.

# Introducción al análisis estático

## Laboratorio de análisis – Arquitectura de red.

En primer lugar deberemos crear dos máquinas virtuales una Windows y otra Linux. La arquitectura de red debe solo permitir la comunicación entre las dos máquinas pero no con el exterior.



---

# Introducción al análisis estático

## Laboratorio de análisis – Arquitectura de red.

Crear un laboratorio de malware es algo muy sencillo. Solo es necesario crear las dos máquinas virtuales y que tengan conexión en una red privada virtual (isolated virtual network).

Una vez instaladas y tengan comunicación a través de esa red privada debemos:

- Crear una instantánea de la imagen Windows y de la imagen Linux. En caso de infección permitirá volver a un estado anterior.
- Configurar el entorno de red.
- Instalar Inetsim en la máquina Linux.
- Instalar todas las herramientas para proceder al análisis en Windows.

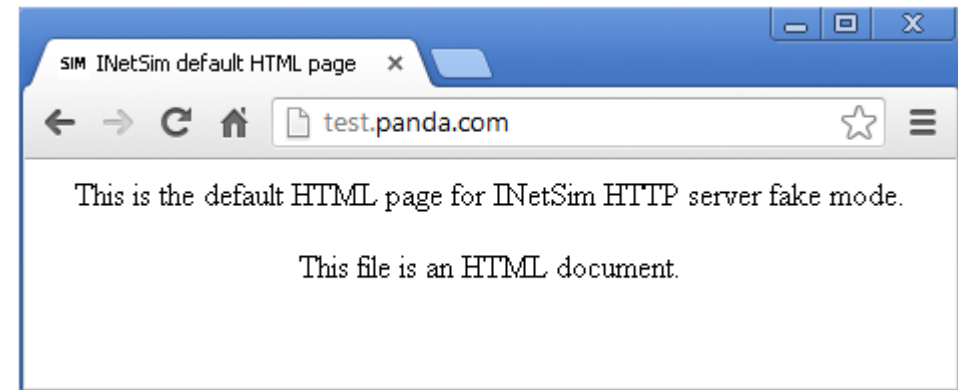
# Introducción al análisis estático

## Laboratorio de análisis – InetSim

InetSim es un software que permite simular los servicios típicos de internet en un entorno de laboratorio para realizar un análisis del comportamiento de red.

Entre los muchos protocolos que permite simular están:

- http/https.
- smtp/smtps.
- Pop3/pop3s.
- ftp/sftp.
- DNS.
- NTP.
- Etc.



---

# Introducción al análisis estático

## Introducción – Análisis estático

El análisis estático describe el proceso de analizar una muestra según la estructura del fichero sin llegar a ejecutarlo.

En esta fase la información a recopilar es:

- Identificación del archivo, hash MD5.
- Motores Antivirus, Virustotal como primera aproximación.
- Obtención de datos acerca del fichero: strings, headers, librerías, etc.

---

# Introducción al análisis estático

## Breve descripción de un PE

Cuando hablamos de un **PE** estamos hablando de un fichero **ejecutable** para OS **Windows**.

El resultado de compilar código se traduce en una estructura de datos, PE, que encapsula toda la información que necesita el loader de Windows para administrar el código del ejecutable.

Esto significa que en el PE habrá información no solo relativa al código compilado sino también:

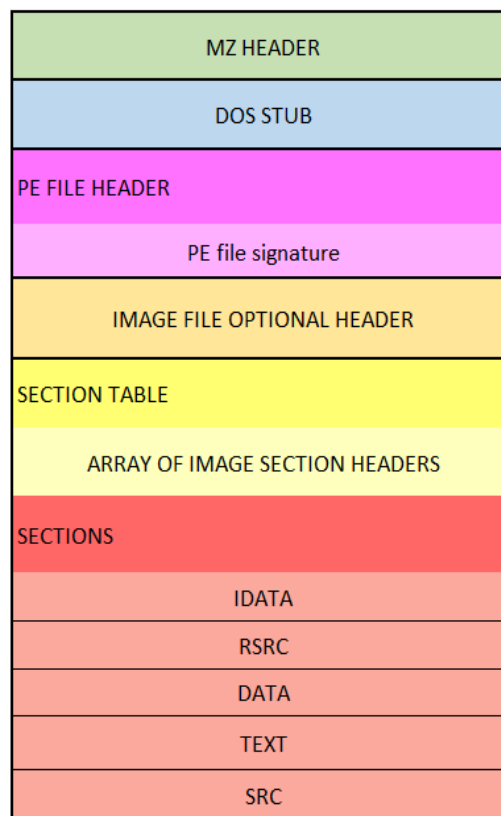
- Identificador de tipo de archivo. Magic number.
- Librerías que necesita el ejecutable.
- Tamaño de fichero en disco y en memoria virtual (en tiempo de ejecución).
- Arquitectura para la que fue compilado (x86 o x64).
- Etc.

---

# Introducción al análisis estático

## Estructura básica de un PE

La estructura de un PE representada de forma gráfica y de forma muy resumida puede entenderse como:



---

# Introducción al análisis estático

## Descripción de la estructura de un PE

La información almacenada en un PE es de mucha utilidad, veamos una pequeña descripción:

- **MZ HEADER.** Se trata de los primeros 64 bytes de todo PE. Contiene, entre otras cosas, el magic number.
  - El **Magic Number** se encuentra en los **dos primeros bytes** del PE y es el identificativo de que tipo de fichero es. Un **PE** empezará siempre con **4D 5A**.
- **Dos Stub** Usualmente suele contener la clásica cadena: *This program cannot be run in DOS mode.*

---

# Introducción al análisis estático

## Descripción de la estructura de un PE

- **PE File Header.** Contiene información relativa al resto de la estructura del fichero:
  - Dirección de memoria donde se encuentra el código.
  - Tamaño del archivo en disco y en memoria virtual.
  - Número de secciones.
  - Dirección de carga cuando el archivo sea mapeado en memoria.
  - Información relativa al alineamiento de las diferentes secciones.
  - Etc.

---

# Introducción al análisis estático

## Descripción de la estructura de un PE

- **Section Table:** Contiene información relativa a las secciones, para cada sección habrá una entrada en la section table.
- **Sections:** Contiene la información referida a recursos que necesita el ejecutable (imágenes, strings, etc), espacio de memoria a escribir en tiempo de ejecución, código, etc.

Aunque hay mucha información interesante la estructura del PE, veremos con un poco más de profundidad las **Sections** dado que están **directamente relacionadas con el código**.

---

# Introducción al análisis estático

## Descripción de la estructura de un PE - Sections

Las secciones típicamente a encontrar en un PE son:

- **.idata:** Almacena los datos relacionados con los imports que el programa necesita. Si una librería del sistema será cargada, aparecerá en la sección idata.
- **.rsrc:** Contiene los recursos necesarios que no son considerados como parte del ejecutable. Se encuentran imágenes, iconos, strings.
- **.data:** Contiene los datos del programa de entorno global. Son datos accesibles desde cualquier parte del programa.
- **.text:** Contiene las instrucciones que serán ejecutadas por la CPU. El resto de secciones contienen datos de apoyo. Es **la única** sección **que debe contener código**.
- **.reloc:** Esta sección entra en juego cuando ejecutamos el programa y hay que emplazar el PE en memoria. Indica cómo deben ser modificadas las direcciones de memoria del PE para mapear en memoria virtual.

---

# Introducción al análisis estático

## Presentación de las herramientas

Estás son algunas de las muchas herramientas para iniciar un análisis:

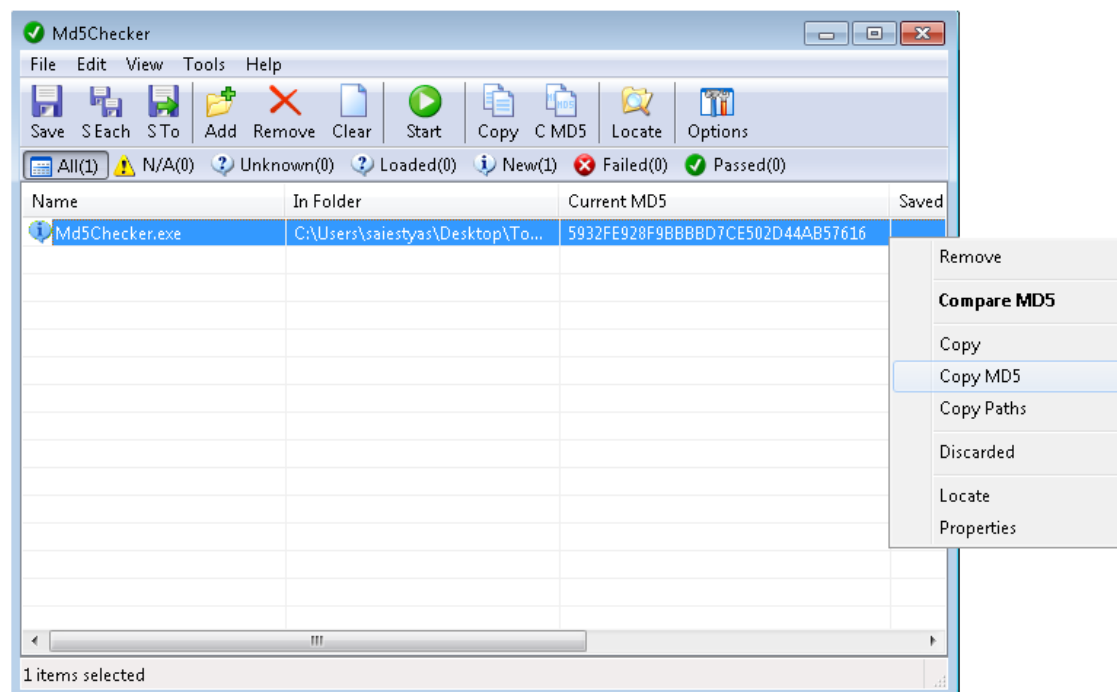
- **MD5Chequer:** Cálculo del hash MD5 del archivo.
- **VirusTotal:** Página web donde se permite analizar ficheros con multitud de motores antivirus de forma gratuita.
- **HxD:** Editor hexadecimal.
- **Strings:** Muestra las cadenas contenidas en el PE. (Microsoft Sysinternals Suite).
- **Die – Detect it easy:** Herramienta que muestra si un archivo ha sido manipulado por un packer.
- **Resource Hacker:** Permite la extracción de recursos (.rsrc section). Se usa para extraer o manipular elementos del programa.
- **PeStudio:** Herramienta para investigar cualquier binario de Windows. Contiene mucha información relativa a las secciones y otros metadatos.

# Introducción al análisis estático

## Presentación de las herramientas - Md5Chequer

Todo archivo objeto de análisis debe ser identificado de forma unívoca. Por ello las muestras son nombradas con su MD5 tanto a nivel profesional como educativo.

La herramienta MD5chequer es prácticamente auto-explicativa:



# Introducción al análisis estático



## Presentación de las herramientas – VirusTotal

VirusTotal es una de las webs más grandes de análisis online y dispone de más de 60 motores antivirus para realizar el análisis. Permite: subida de ficheros, análisis de urls o búsqueda de cadenas que identifiquen al archivo que queremos analizar.



Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.

File	URL	Search
------	-----	--------

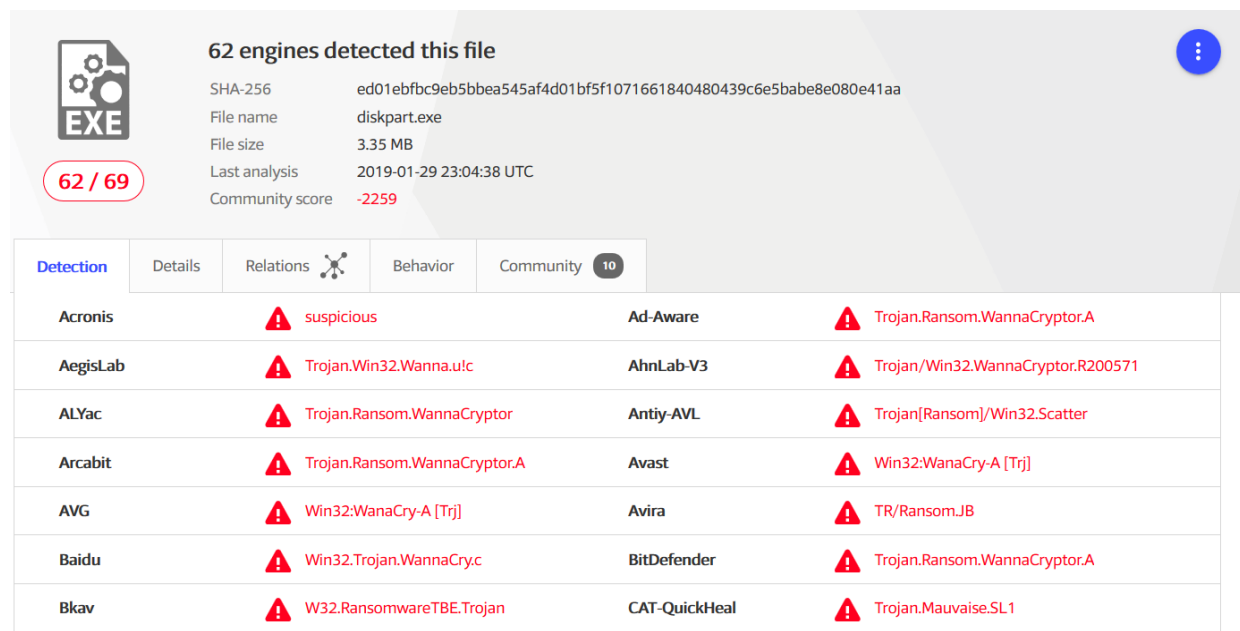
  
  
  

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#).

# Introducción al análisis estático

## Presentación de las herramientas – Virustotal ejemplo de detección

En este caso se ha introducido el MD5 de un malware relacionado con el famoso ataque WannaCry.



62 engines detected this file

SHA-256 ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa  
File name diskpart.exe  
File size 3.35 MB  
Last analysis 2019-01-29 23:04:38 UTC  
Community score -2259

62 / 69

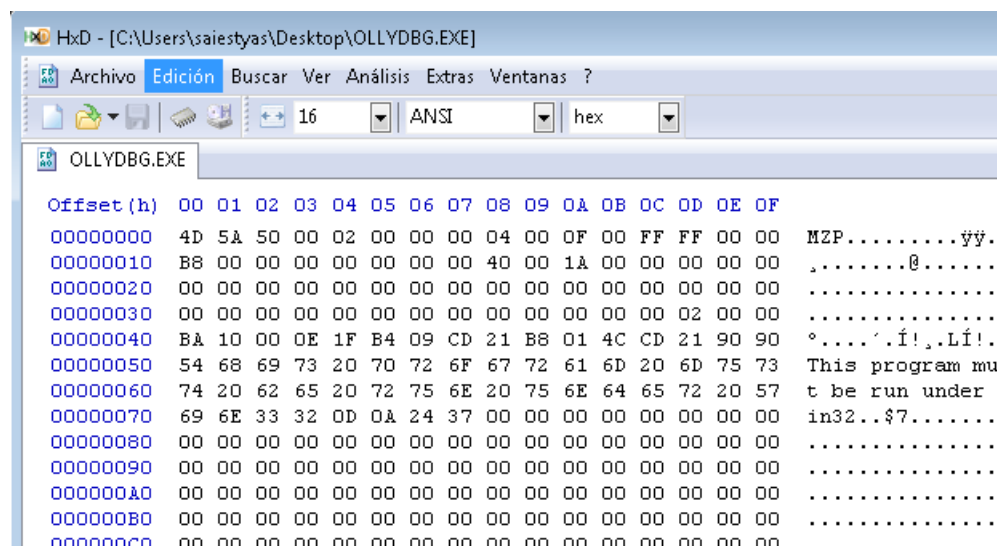
Detection Details Relations Behavior Community 10

Acronis	⚠ suspicious	Ad-Aware	⚠ Trojan.Ransom.WannaCryptor.A
AegisLab	⚠ Trojan.Win32.Wanna.u!c	AhnLab-V3	⚠ Trojan/Win32.WannaCryptor.R200571
ALYac	⚠ Trojan.Ransom.WannaCryptor	Antiy-AVL	⚠ Trojan[Ransom]/Win32.Scatter
Arcabit	⚠ Trojan.Ransom.WannaCryptor.A	Avast	⚠ Win32:WanaCry-A [Trj]
AVG	⚠ Win32:WanaCry-A [Trj]	Avira	⚠ TR/Ransom.JB
Baidu	⚠ Win32.Trojan.WannaCry.c	BitDefender	⚠ Trojan.Ransom.WannaCryptor.A
Bkav	⚠ W32.Ransomware.TBE.Trojan	CAT-QuickHeal	⚠ Trojan.Mauvaise.SL1

# Introducción al análisis estático

## Presentación de las herramientas – Editor hexadecimal

HxD es uno de tantos editores hexadecimales gratuitos. Dada su simplicidad de uso es objeto de uso:



Puede ser muy útil a la hora de buscar cadenas concretas a primer ojo o cuando queremos modificar bytes del archivo.

# Introducción al análisis estático

## Presentación de las herramientas – Strings

El programa strings pertenece a las **Sysinternals suite** ofrecida por **Microsoft**.

En las Sysinternals Suite encontramos utilidades dirigidas a diagnóstico, traza de errores, monitorización, etc.

Tal y como su propio nombre indica Strings extrae las cadenas en formato ASCII o UNICODE de un PE, permitiéndonos almacenar su contenido en un fichero para su posterior análisis:

```
ca: C:\Windows\system32\cmd.exe
C:\Users\saiestyas\Desktop>strings OLLYDBG.EXE >> test.txt
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
.exe;*.dll|.obj;*.lib
.c;*.cpp;*.h;*.hpp;*.asm;*.pas|.c;*.cpp|.h;*.hpp|.asm|.pas|.txt|.bak
You have changed the command line arguments. If you want that new
arguments take effect now, you must restart debugged program.
Command line arguments changed
Please select directory containing files with symbolic debugging
data:
Select API help file
Settings
Unable to write back modified registers
Unrecoverable breakpoint at %08lX
OllyDbg is unable to read registers and update EIP for breakpoint at
(possibly invalid) address %08lX. This usually makes correct
```

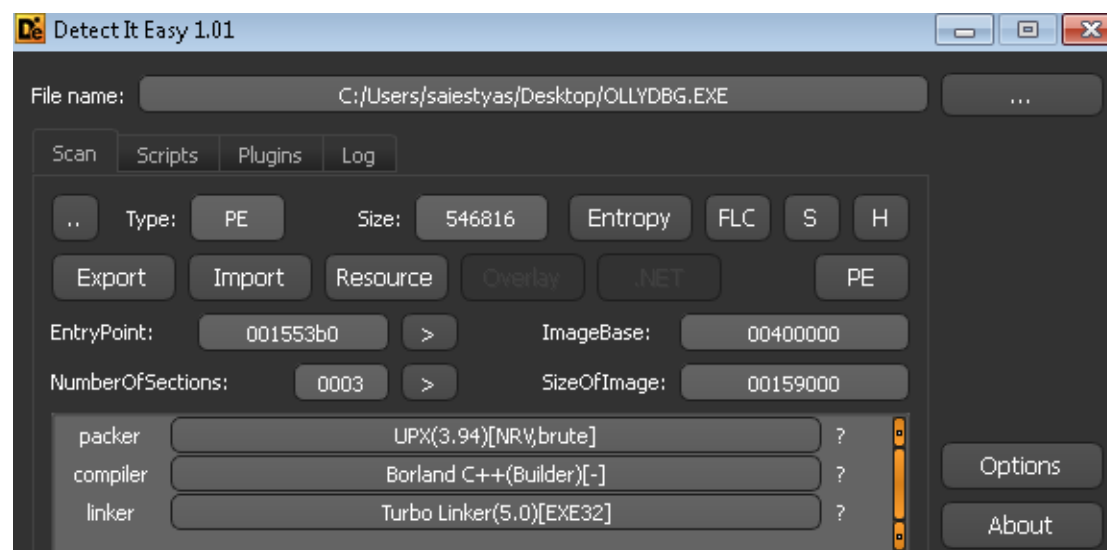
# Introducción al análisis estático

## Presentación de las herramientas – Detect it Easy (DiE)

En muchas ocasiones los programas tanto maliciosos como no maliciosos son protegidos con capas de cifrado y también de ofuscación.

DiE es capaz de distinguir entre un gran abanico de packers junto con su versión.

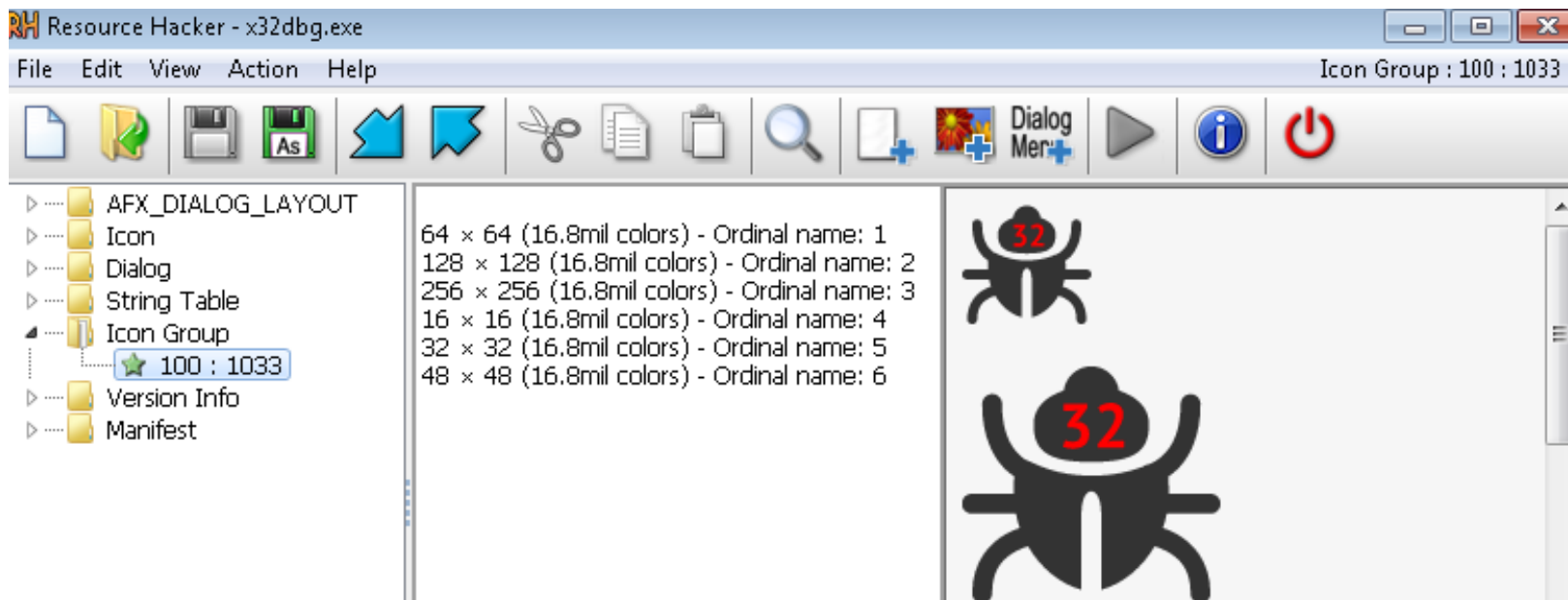
Los packers son esos programas que se encargan de introducir esa capa/s de cifrado u ofuscación.



# Introducción al análisis estático

## Presentación de las herramientas - Resource Hacker

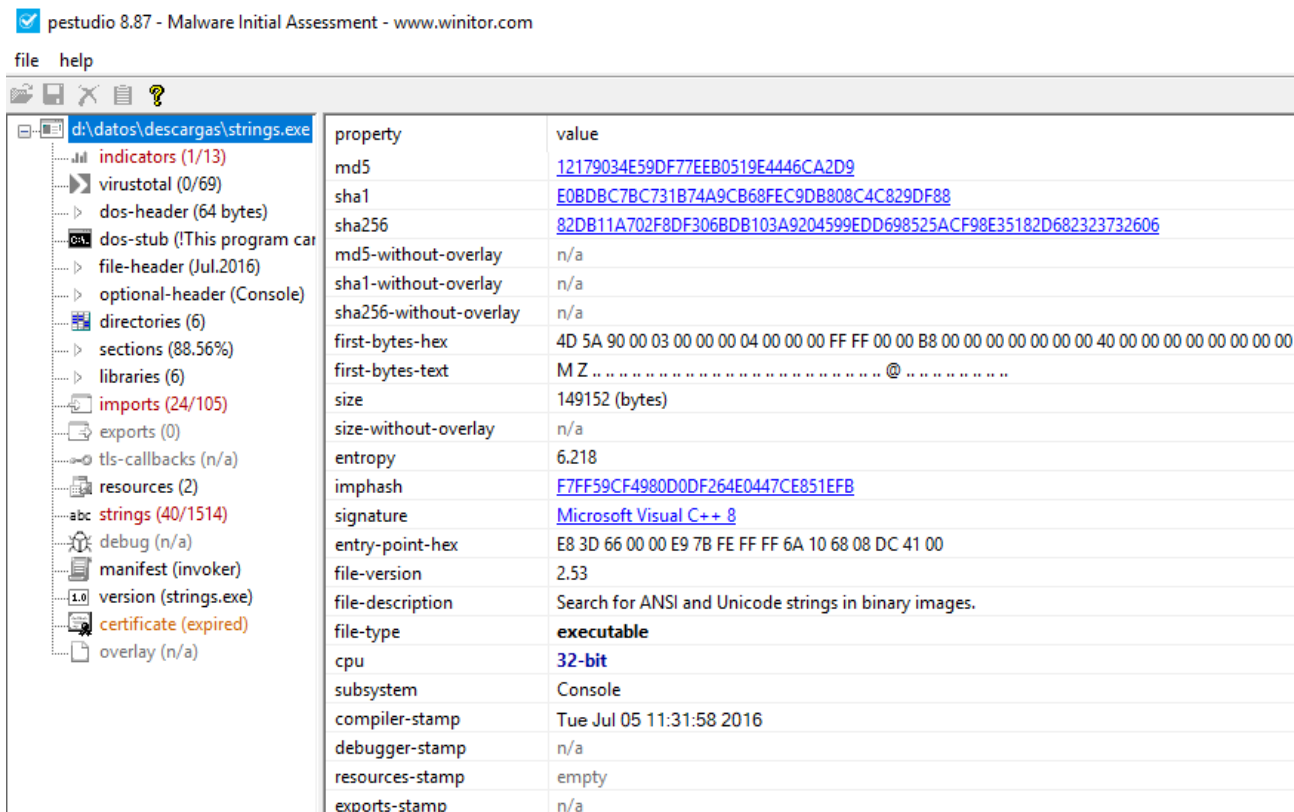
Resource Hacker es una herramienta útil con la que podemos: ver, extraer e incluso modificar recursos (.rsrc) de un PE.



# Introducción al análisis estático

## Presentación de las herramientas - PeStudio Visión general

PeStudio es una gran herramienta que aglutina funcionalidades de otras ofreciendo en un solo programa una gran suite de herramientas para el visionado de metadatos del PE.



pestudio 8.87 - Malware Initial Assessment - www.winator.com

file help

d:\datos\descargas\strings.exe

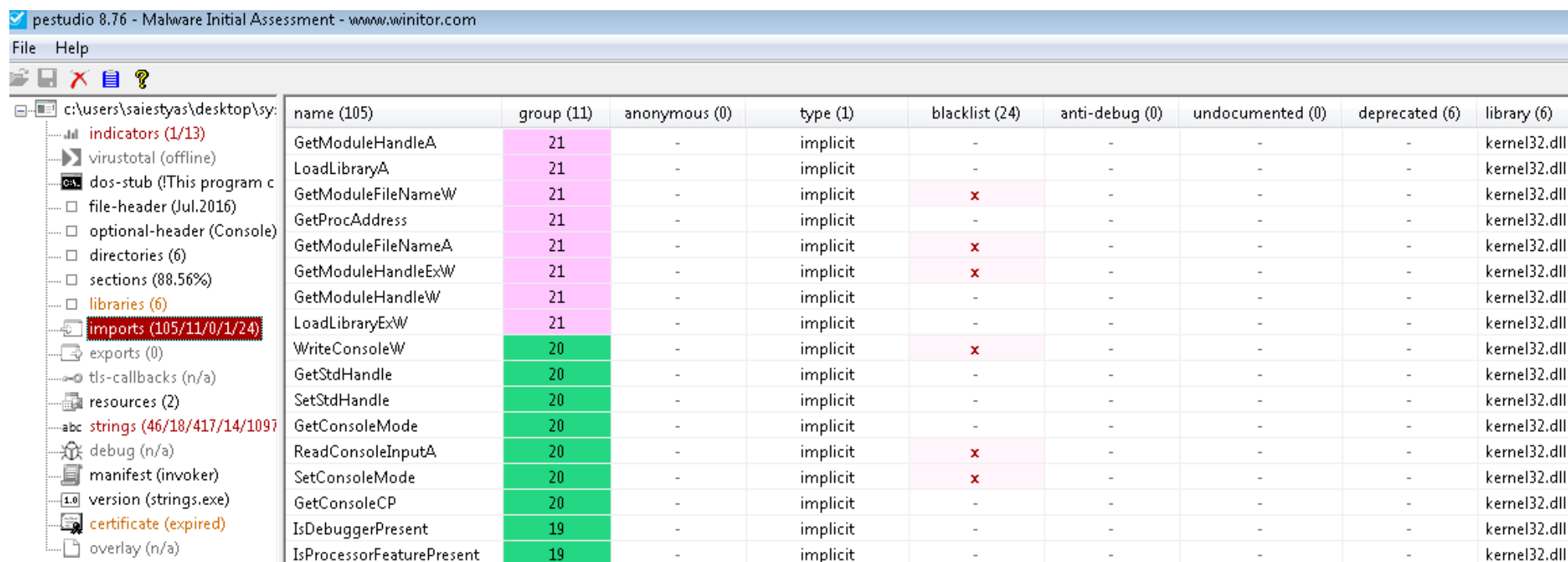
property	value
md5	<a href="#">12179034E59DF77EEB0519E4446CA2D9</a>
sha1	<a href="#">E0BDBC7BC731B74A9CB68FEC9DB808C4C829DF88</a>
sha256	<a href="#">82DB11A702F8DF306BDB103A9204599EDD698525ACF98E35182D682323732606</a>
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
size	149152 (bytes)
size-without-overlay	n/a
entropy	6.218
imphash	<a href="#">F7FF59CF4980D0DF264E0447CE851EFB</a>
signature	<a href="#">Microsoft Visual C++ 8</a>
entry-point-hex	E8 3D 66 00 00 E9 7B FE FF FF 6A 10 68 08 DC 41 00
file-version	2.53
file-description	Search for ANSI and Unicode strings in binary images.
file-type	<b>executable</b>
cpu	<b>32-bit</b>
subsystem	Console
compiler-stamp	Tue Jul 05 11:31:58 2016
debugger-stamp	n/a
resources-stamp	empty
exports-stamp	n/a

# Introducción al análisis estático

## Presentación de las herramientas - PeStudio – Imports y Exports

En el apartado **imports** podemos ver todas las **llamadas a funciones** de **librerías externas** realizadas por el programa. Esto puede ser un gran indicador puesto que en el caso que nos ocupa ahora

¿Qué implicaría una llamada a GetConnection?



name (105)	group (11)	anonymous (0)	type (1)	blacklist (24)	anti-debug (0)	undocumented (0)	deprecated (6)	library (6)
GetModuleHandleA	21	-	implicit	-	-	-	-	kernel32.dll
LoadLibraryA	21	-	implicit	-	-	-	-	kernel32.dll
GetModuleFileNameW	21	-	implicit	x	-	-	-	kernel32.dll
GetProcAddress	21	-	implicit	-	-	-	-	kernel32.dll
GetModuleFileNameA	21	-	implicit	x	-	-	-	kernel32.dll
GetModuleHandleExW	21	-	implicit	x	-	-	-	kernel32.dll
GetModuleHandleW	21	-	implicit	-	-	-	-	kernel32.dll
LoadLibraryExW	21	-	implicit	-	-	-	-	kernel32.dll
WriteConsoleW	20	-	implicit	x	-	-	-	kernel32.dll
GetStdHandle	20	-	implicit	-	-	-	-	kernel32.dll
SetStdHandle	20	-	implicit	-	-	-	-	kernel32.dll
GetConsoleMode	20	-	implicit	-	-	-	-	kernel32.dll
ReadConsoleInputA	20	-	implicit	x	-	-	-	kernel32.dll
SetConsoleMode	20	-	implicit	x	-	-	-	kernel32.dll
GetConsoleCP	20	-	implicit	-	-	-	-	kernel32.dll
IsDebuggerPresent	19	-	implicit	-	-	-	-	kernel32.dll
IsProcessorFeaturePresent	19	-	implicit	-	-	-	-	kernel32.dll

---

# Introducción al análisis estático

## Presentación de las herramientas - PeStudio – Imports reseñables

KERNEL32.dll	Acceso y manipulación de memoria, archivos, creación de procesos y hardware.
Advapi32.dll	Relacionado con operaciones de registro y administración de servicios.
User32.dll	Componentes de interfaz de usuario (GUI).
Ntdll.dll	Interface con el kernel de Windows.
WSock32.dll y Ws2_32.dll	Acceso a operaciones de red.
Wininet.dll	Alto nivel de red, tales como protocolos HTTP, FTP y NTP.

# Introducción al análisis estático

## Presentación de las herramientas - PeStudio – Funciones reseñables

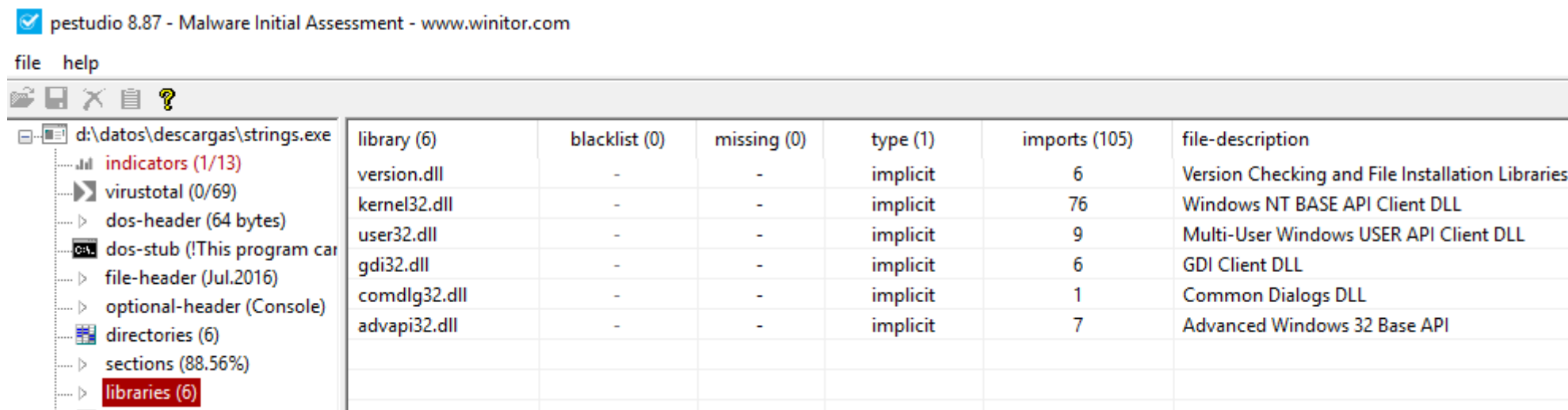
CreateProcess	Usadas para crear procesos / threads nuevos
CreateThread	
CreateToolhelp32Snapshot	Crea un snapshot de los procesos con su memoria, módulos y threads utilizados
Process32Next	Utilizada conjunto la anterior, itera entre los procesos del snapshot
EnumProcesses	Enumera los procesos actuales del sistema
CryptAcquireContext	Utilizada para inicializar el cifrado de Windows
FindResource	Busca un recurso en la sección .rsrc
CreateMutex	Crea un objeto exclusivo para asegurar que solo se ejecuta una instancia del programa
AdjustTokenPrivileges	Ajusta los privilegios del proceso
FindWindow	Busca el nombre de alguna en las ventanas abiertas
GetAsyncKeyState	Funciones para obtener el estado del teclado
GetKeyState	
GetTempPath	Obtienes el path del directorio %TEMP%
inet_addr	Convierte strings de IP en objetos útiles
InternetOpen	Inicia las funciones WinINet
InternetWriteFile/ReadFile	Escribe/lee información abierta por las funciones de WinINet

# Introducción al análisis estático

## Presentación de las herramientas - PeStudio – Libraries

Si con los imports y exports se observaban las llamadas a funciones de librerías, en libraries veremos solo las librerías que carga el PE.

De este modo si apareciera una librería que no cuadra con el contexto del programa podemos encontrar IOCS. le contener llamadas a la librería winsock.



library (6)	blacklist (0)	missing (0)	type (1)	imports (105)	file-description
version.dll	-	-	implicit	6	Version Checking and File Installation Libraries
kernel32.dll	-	-	implicit	76	Windows NT BASE API Client DLL
user32.dll	-	-	implicit	9	Multi-User Windows USER API Client DLL
gdi32.dll	-	-	implicit	6	GDI Client DLL
comdlg32.dll	-	-	implicit	1	Common Dialogs DLL
advapi32.dll	-	-	implicit	7	Advanced Windows 32 Base API

# Introducción al análisis estático

## Presentación de las herramientas - PeStudio – Sections

Quizás uno de los apartados más importantes a revisar. Podemos ver:

- Permisos de R/W/X
- Hash Md5
- Nivel de compresión
- Etc.

pestudio 8.87 - Malware Initial Assessment - www.winitor.com

file help

d:\datos\descargas\strings.exe

- indicators (1/13)
- virusotal (0/69)
- dos-header (64 bytes)
- dos-stub (This program can't be opened. Your computer may not have enough memory to open the file, or the file may have moved. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the file and then insert it again.)
- file-header (Jul.2016)
- optional-header (Console)
- directories (6)
- sections (88.56%)**
- libraries (6)
- imports (24/105)
- exports (0)
- tls-callbacks (n/a)
- resources (2)
- strings (40/1514)
- debug (n/a)
- manifest (invoker)
- version (strings.exe)
- certificate (expired)
- overlay (n/a)

property	value	value	value	value	value
name	.text	.rdata	.data	.rsrc	.reloc
md5	5A345F4BB5E0A5715EAC261...	2695882EDB933E070C2FEB9...	5743D7D4483064E89C3FC0F...	B7ADF8911EC0ACC6784078...	C27E2CFB5586001E25693056...
file-ratio (88.56 %)	49.09 %	31.92 %	3.43 %	1.03 %	3.09 %
virtual-size (138560 bytes)	0x00011C74 (72820 bytes)	0x0000B8EC (47340 bytes)	0x00003128 (12584 bytes)	0x00000588 (1416 bytes)	0x00001130 (4400 bytes)
raw-size (132096 bytes)	0x00011E00 (73216 bytes)	0x0000BA00 (47616 bytes)	0x00001400 (5120 bytes)	0x00000600 (1536 bytes)	0x00001200 (4608 bytes)
file-cave (1000 bytes)	396 bytes	276 bytes	0 bytes	120 bytes	208 bytes
virtual-address	0x00401000	0x00413000	0x0041F000	0x00423000	0x00424000
raw-address	0x00000400	0x00012200	0x0001DC00	0x0001F000	0x0001F600
entropy	6.590	4.658	3.316	3.903	6.521
entry-point (0x000058A6)	x	-	-	-	-
writable	-	-	x	-	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
readable	x	x	x	x	x
self-modifying	-	-	-	-	-

---

# Introducción al análisis estático

## Presentación de las herramientas - PeStudio – Otros datos relevantes

PeStudio es una herramienta muy versátil y la información que contiene es muy extensa algunos de los apartados que han quedado atrás pero también relevantes son:

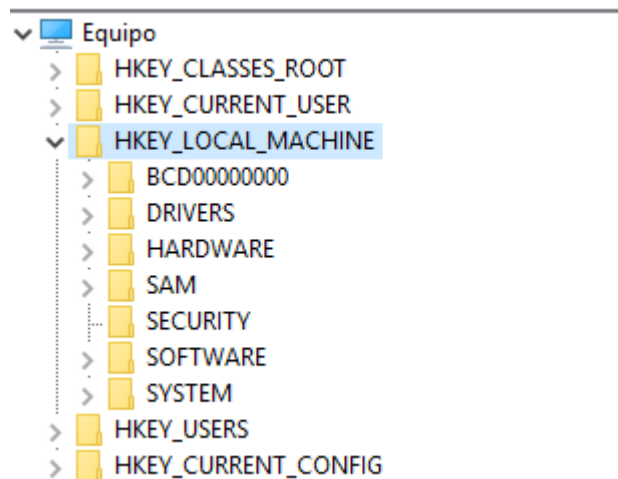
- Strings
- Version
- Overlay
- Debug
- Resources

¿Y todas las herramientas anteriores? PeStudio aglutina a todas ellas, ¿Significa eso que podemos prescindir de ellas y solo usar PeStudio?

# Introducción al análisis dinámico

## Pequeño resumen del funcionamiento de Windows – Windows Registry

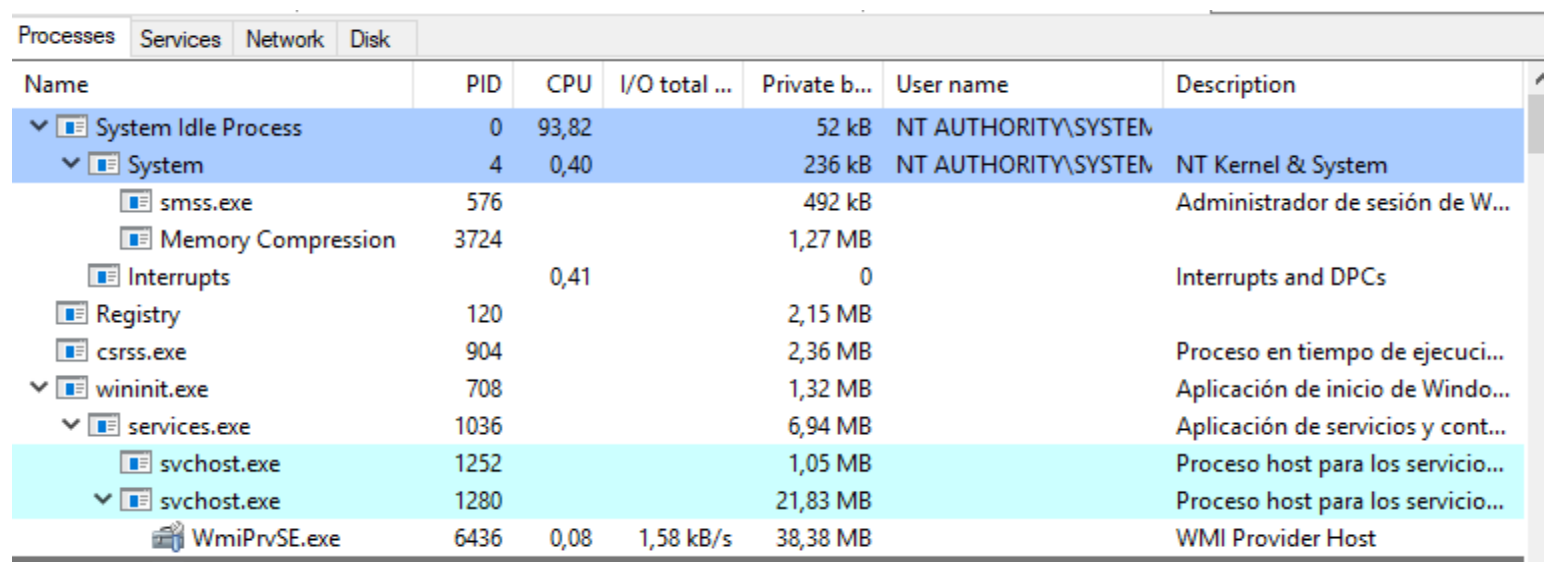
- Se trata de una base de datos utilizada para almacenar información de configuración y opciones de componentes de Windows y también aplicaciones de terceros.
- El malware utiliza el registro comúnmente para obtener persistencia en el sistema, obtener información del ordenador, establecer datos de configuración, etc.
- Buen lugar para obtener indicadores de compromiso.



# Introducción al análisis dinámico

## Pequeño resumen del funcionamiento de Windows – Procesos

- Todo el sistema operativo basa su funcionamiento en la ejecución de los procesos, que corresponden a las aplicaciones y servicios que se ejecuta en cada momento.
- Los procesos contienen en memoria el mapeado de cada una de las secciones del PE, el sistema operativo se encarga de preparar la memoria para su correcta ejecución.
- Existe malware que puede inyectarse en la memoria de otros procesos o en procesos nuevos creados,



Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	93,82		52 kB	NT AUTHORITY\SYSTEM	
System	4	0,40		236 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	576			492 kB		Administrador de sesión de W...
Memory Compression	3724			1,27 MB		
Interrupts		0,41		0		Interrupts and DPCs
Registry	120			2,15 MB		
csrss.exe	904			2,36 MB		Proceso en tiempo de ejecuci...
wininit.exe	708			1,32 MB		Aplicación de inicio de Windo...
services.exe	1036			6,94 MB		Aplicación de servicios y cont...
svchost.exe	1252			1,05 MB		Proceso host para los servicio...
svchost.exe	1280			21,83 MB		Proceso host para los servicio...
WmiPrvSE.exe	6436	0,08	1,58 kB/s	38,38 MB		WMI Provider Host

# Introducción al análisis dinámico

## Pequeño resumen del funcionamiento de Windows – Procesos comunes

<b>svchost.exe</b>	nombre genérico de proceso anfitrión para servicios
<b>lsass.exe</b>	responsable de cumplir la política de seguridad en el sistema
<b>services.exe</b>	inicia, detiene e interactúa con procesos de servicios de Windows
<b>winlogon.exe</b>	carga el perfil de usuario, bloqueo del sistema, verificación de las credenciales de usuario
<b>csrss.exe</b>	encargado de la consola de windows y del proceso de apagado de la GUI
<b>Smss.exe</b>	ejecutado durante el proceso de arranque, tiene como hijos winlogon.exe y csrss.exe (entre otros)
<b>ntvdm.exe</b>	permite ejecutar MS-DOS aplicaciones en ordenadores actuales

---

# Introducción al análisis dinámico

## Introducción – Análisis dinámico

El análisis dinámico describe el proceso de analizar una muestra según su comportamiento durante la ejecución.

La información importante a recopilar es:

- Uso de red, tanto conexiones internas como externas.
- Creación o cualquier tipo de manipulación de ficheros.
- Carga o uso de elementos no visibles durante el análisis estático.
- Interacción con el sistema de ficheros.
- Cambios en los procesos de ejecución.
- Etc.

---

# Introducción al análisis dinámico

## Presentación de las herramientas - Clasificación

Existen diferentes tipos de herramientas para el análisis dinámico pero en su gran mayoría se pueden dividir en 3 grupos según su funcionamiento:

- Herramienta de análisis basadas en Hooks.
- Herramientas basadas en la diferencia o variación.
- Herramientas basadas en las notificaciones.

# Introducción al análisis dinámico

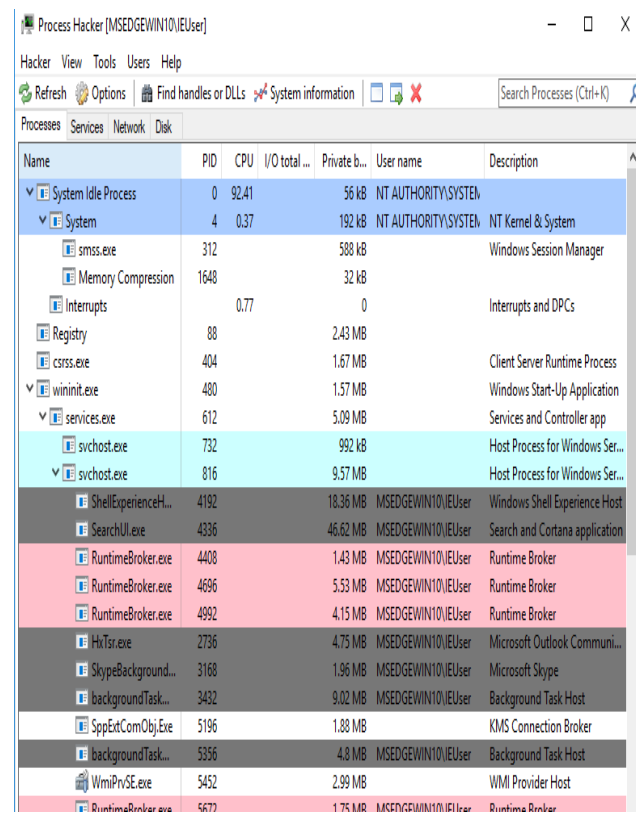
## Presentación de las herramientas - Herramienta de análisis basadas en hooks

Estas herramientas interceptan las llamadas a las funciones o los elementos del sistema para monitorizar en tiempo real, tanto a nivel de usuario como de sistema.

Se pueden observar:

- Conexiones de red.
- Árbol de procesos.
- Interacción con el sistema de archivos.
- Servicios activos.

Ej, Process Hacker, SysAnalysis.



The screenshot shows the Process Hacker application window. The title bar reads "Process Hacker [MSEdgeWin10\IEUser]". The menu bar includes "Hacker", "View", "Tools", "Users", and "Help". The toolbar contains icons for "Refresh", "Options", "Find handles or DLLs", "System information", and a search icon. The search bar contains the text "Search Processes (Ctrl+K)". The main window displays a table of processes with columns for Name, PID, CPU, I/O total, Private b..., User name, and Description. The table is expanded to show the "System" process, which includes sub-processes like "smss.exe", "Memory Compression", "Interrupts", "Registry", "csrss.exe", "winit.exe", "services.exe", and "svchost.exe". The "svchost.exe" process is highlighted in blue, and its sub-processes are also highlighted in blue. Other processes like "ShellExperienceHost.exe", "SearchUI.exe", "RuntimeBroker.exe", "HxTsr.exe", "SkypeBackgroundTaskHost.exe", "backgroundTaskHost.exe", "SppExtComObj.exe", "backgroundTaskHost.exe", "WmiPrvSE.exe", and "RuntimeBroker.exe" are also visible in the list.

Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	92.41		56 kB	NT AUTHORITY\SYSTEM	
System	4	0.37		192 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	312			588 kB		Windows Session Manager
Memory Compression	1648			32 kB		
Interrupts		0.77		0		Interrupts and DPCs
Registry	88			2.43 MB		
csrss.exe	404			1.67 MB		Client Server Runtime Process
winit.exe	480			1.57 MB		Windows Start-Up Application
services.exe	612			5.09 MB		Services and Controller app
svchost.exe	732			992 kB		Host Process for Windows Ser...
svchost.exe	816			9.57 MB		Host Process for Windows Ser...
ShellExperienceH...	4192			18.36 MB	MSEdgeWin10\IEUser	Windows Shell Experience Host
SearchUI.exe	4336			46.62 MB	MSEdgeWin10\IEUser	Search and Cortana application
RuntimeBroker.exe	4408			1.43 MB	MSEdgeWin10\IEUser	Runtime Broker
RuntimeBroker.exe	4696			5.53 MB	MSEdgeWin10\IEUser	Runtime Broker
RuntimeBroker.exe	4892			4.15 MB	MSEdgeWin10\IEUser	Runtime Broker
HxTsr.exe	2736			4.75 MB	MSEdgeWin10\IEUser	Microsoft Outlook Communi...
SkypeBackground...	3168			1.96 MB	MSEdgeWin10\IEUser	Microsoft Skype
backgroundTask...	3432			9.02 MB	MSEdgeWin10\IEUser	Background Task Host
SppExtComObj.Exe	5196			1.88 MB		KMS Connection Broker
backgroundTask...	5356			4.8 MB	MSEdgeWin10\IEUser	Background Task Host
WmiPrvSE.exe	5452			2.99 MB		WMI Provider Host
RuntimeBroker.exe	5672			1.75 MB	MSEdgeWin10\IEUser	Runtime Broker

# Introducción al análisis dinámico

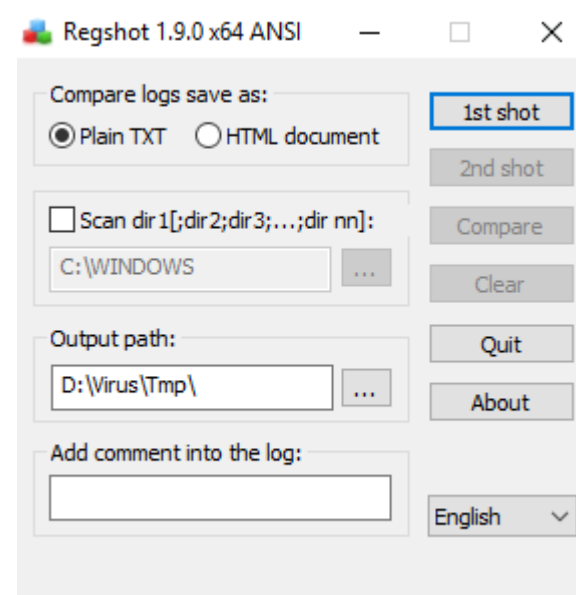
## Presentación de las herramientas - Herramientas basadas en la diferencia

Se encargan de realizar la captura del estado del sistema antes y después de la ejecución del archivo para comprobar las diferencias entre el estado anterior y posterior.

Se pueden observar:

- Cambios en las claves de registro.

Ej, Regshot.



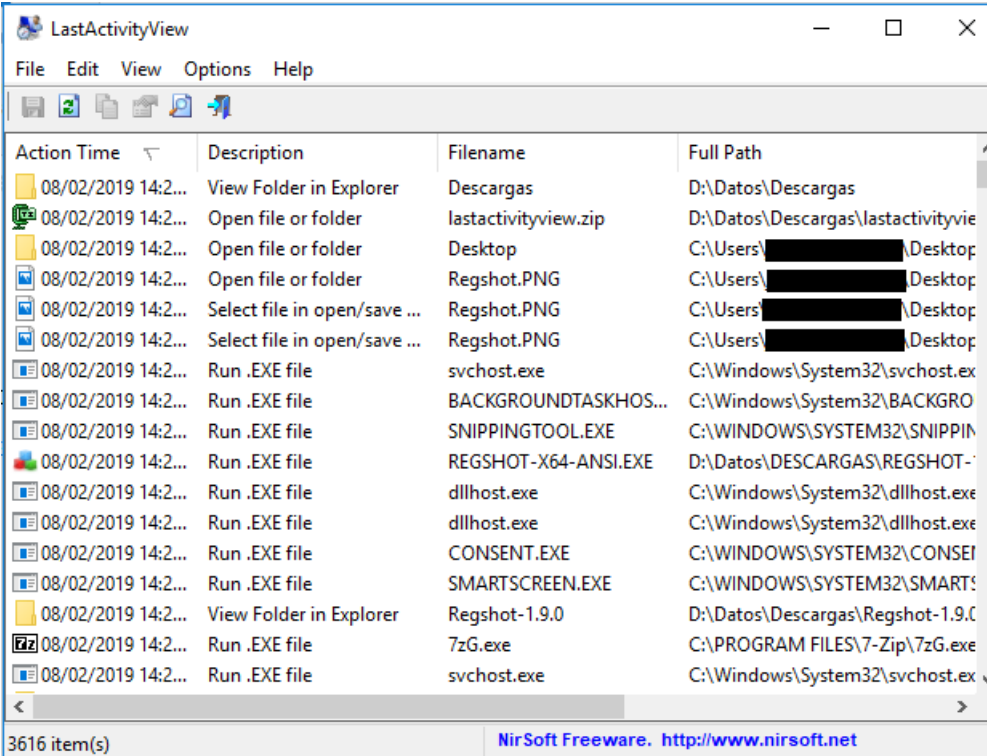
# Introducción al análisis dinámico

## Presentación de las herramientas - Herramientas basadas en las notificaciones

Estas herramientas registran las rutinas de notificación del sistema cuando suceden una serie de eventos. Se utilizan comúnmente para realizar análisis forense

La diferencia con las herramientas de hooks radica en que estas registran los eventos propios del sistema.

Ej, LastActivityView.



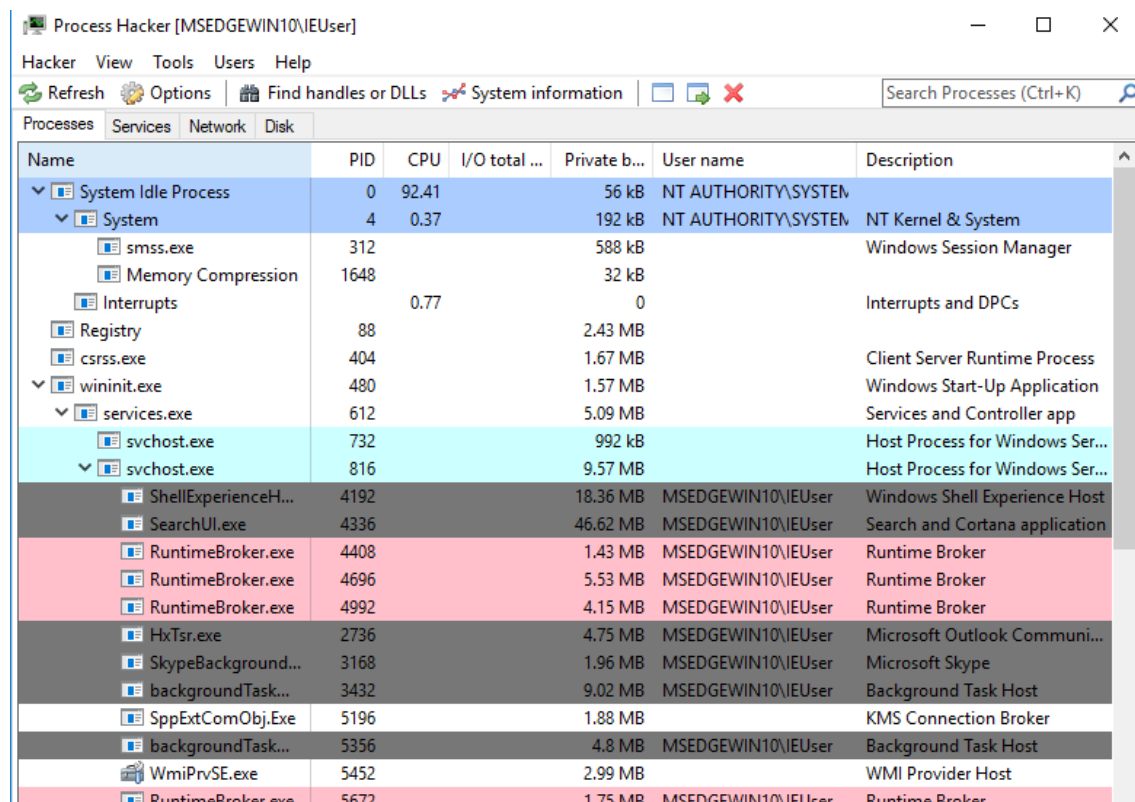
The screenshot shows the LastActivityView application window. The window title is "LastActivityView" and it has a menu bar with "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area contains a table with the following columns: "Action Time", "Description", "Filename", and "Full Path". The table lists various system events, including file operations, running .EXE files, and viewing folders in Explorer. The status bar at the bottom indicates "3616 item(s)" and includes a link to "NirSoft Freeware. http://www.nirsoft.net".

Action Time	Description	Filename	Full Path
08/02/2019 14:2...	View Folder in Explorer	Descargas	D:\Datos\Descargas
08/02/2019 14:2...	Open file or folder	lastactivityview.zip	D:\Datos\Descargas\lastactivityvie
08/02/2019 14:2...	Open file or folder	Desktop	C:\Users\[redacted]\Desktop
08/02/2019 14:2...	Open file or folder	Regshot.PNG	C:\Users\[redacted]\Desktop
08/02/2019 14:2...	Select file in open/save ...	Regshot.PNG	C:\Users\[redacted]\Desktop
08/02/2019 14:2...	Select file in open/save ...	Regshot.PNG	C:\Users\[redacted]\Desktop
08/02/2019 14:2...	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.ex
08/02/2019 14:2...	Run .EXE file	BACKGROUNDTASKHOS...	C:\Windows\System32\BACKGRO
08/02/2019 14:2...	Run .EXE file	SNIPPINGTOOL.EXE	C:\WINDOWS\SYSTEM32\SNIPPIN
08/02/2019 14:2...	Run .EXE file	REGSHOT-X64-ANSI.EXE	D:\Datos\DESCARGAS\REGSHOT-
08/02/2019 14:2...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe
08/02/2019 14:2...	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe
08/02/2019 14:2...	Run .EXE file	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSEI
08/02/2019 14:2...	Run .EXE file	SMARTSCREEN.EXE	C:\WINDOWS\SYSTEM32\SMARTS
08/02/2019 14:2...	View Folder in Explorer	Regshot-1.9.0	D:\Datos\Descargas\Regshot-1.9.0
08/02/2019 14:2...	Run .EXE file	7zG.exe	C:\PROGRAM FILES\7-Zip\7zG.exe
08/02/2019 14:2...	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.ex

# Introducción al análisis dinámico

## Presentación de las herramientas - Process Hacker

Gracias a esta herramienta se puede hacer un primer modelaje de comportamiento dada la información que ofrece. Además es capaz de mostrar información relevante como los permisos, el contenido de la memoria, los threads abiertos, etc.



The screenshot shows the Process Hacker application window. The title bar reads "Process Hacker [MSEDGEWIN10\IEUser]". The menu bar includes "Hacker", "View", "Tools", "Users", and "Help". Below the menu bar is a toolbar with icons for "Refresh", "Options", "Find handles or DLLs", "System information", and a search icon. A search box contains the text "Search Processes (Ctrl+K)".

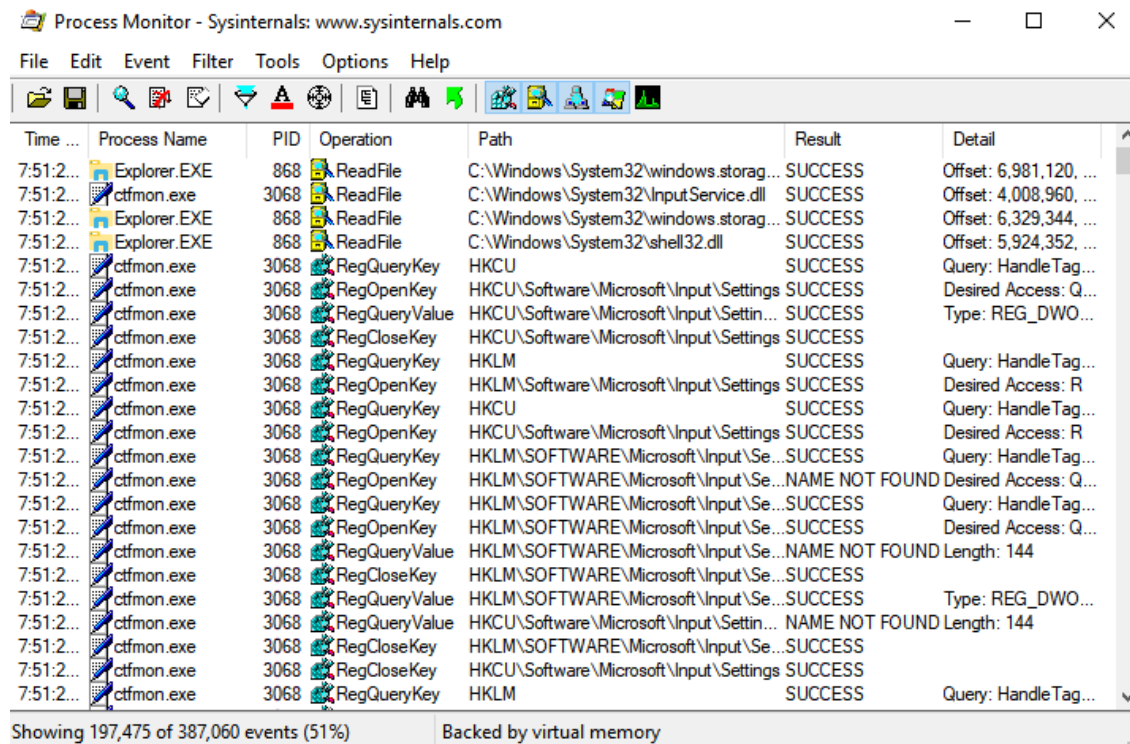
The main window displays a table of processes. The table has columns for "Name", "PID", "CPU", "I/O total ...", "Private b...", "User name", and "Description". The processes are listed in a tree view, with "System Idle Process" at the top, followed by "System", "smss.exe", "Memory Compression", "Interrupts", "Registry", "csrss.exe", "wininit.exe", "services.exe", "svchost.exe", "ShellExperienceH...", "SearchUI.exe", "RuntimeBroker.exe", "HxTsr.exe", "SkypeBackground...", "backgroundTask...", "SppExtComObj.Exe", "backgroundTask...", "WmiPrvSE.exe", and "RuntimeBroker.exe".

Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	92.41		56 kB	NT AUTHORITY\SYSTEM	
System	4	0.37		192 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	312			588 kB		Windows Session Manager
Memory Compression	1648			32 kB		
Interrupts		0.77		0		Interrupts and DPCs
Registry	88			2.43 MB		
csrss.exe	404			1.67 MB		Client Server Runtime Process
wininit.exe	480			1.57 MB		Windows Start-Up Application
services.exe	612			5.09 MB		Services and Controller app
svchost.exe	732			992 kB		Host Process for Windows Ser...
svchost.exe	816			9.57 MB		Host Process for Windows Ser...
ShellExperienceH...	4192			18.36 MB	MSEDGEWIN10\IEUser	Windows Shell Experience Host
SearchUI.exe	4336			46.62 MB	MSEDGEWIN10\IEUser	Search and Cortana application
RuntimeBroker.exe	4408			1.43 MB	MSEDGEWIN10\IEUser	Runtime Broker
RuntimeBroker.exe	4696			5.53 MB	MSEDGEWIN10\IEUser	Runtime Broker
RuntimeBroker.exe	4992			4.15 MB	MSEDGEWIN10\IEUser	Runtime Broker
HxTsr.exe	2736			4.75 MB	MSEDGEWIN10\IEUser	Microsoft Outlook Communi...
SkypeBackground...	3168			1.96 MB	MSEDGEWIN10\IEUser	Microsoft Skype
backgroundTask...	3432			9.02 MB	MSEDGEWIN10\IEUser	Background Task Host
SppExtComObj.Exe	5196			1.88 MB		KMS Connection Broker
backgroundTask...	5356			4.8 MB	MSEDGEWIN10\IEUser	Background Task Host
WmiPrvSE.exe	5452			2.99 MB		WMI Provider Host
RuntimeBroker.exe	5672			1.75 MB	MSEDGEWIN10\IEUser	Runtime Broker

# Introducción al análisis dinámico

## Presentación de las herramientas – Process Monitor

Esta herramienta esta incluida en la Sysinternals Suite de Microsoft, se trata de una herramienta que captura todos los eventos del registro, sistema de ficheros, red y actividad de threads y procesos.



The screenshot shows the Process Monitor application window with a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar. The main area displays a table of system events. The table has columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The events listed are primarily file reads and registry operations performed by Explorer.EXE and ctfmon.exe.

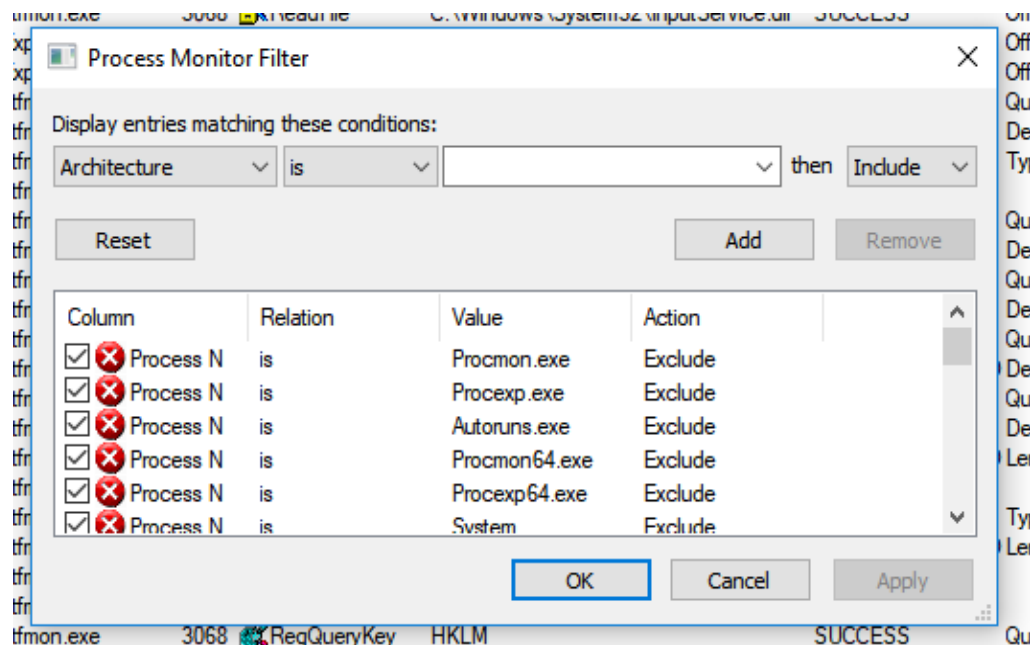
Time ...	Process Name	PID	Operation	Path	Result	Detail
7:51:2...	Explorer.EXE	868	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6,981,120, ...
7:51:2...	ctfmon.exe	3068	ReadFile	C:\Windows\System32\inputService.dll	SUCCESS	Offset: 4,008,960, ...
7:51:2...	Explorer.EXE	868	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6,329,344, ...
7:51:2...	Explorer.EXE	868	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 5,924,352, ...
7:51:2...	ctfmon.exe	3068	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
7:51:2...	ctfmon.exe	3068	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Q...
7:51:2...	ctfmon.exe	3068	RegQueryValue	HKCU\Software\Microsoft\Input\Settin...	SUCCESS	Type: REG_DWO...
7:51:2...	ctfmon.exe	3068	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
7:51:2...	ctfmon.exe	3068	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
7:51:2...	ctfmon.exe	3068	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R
7:51:2...	ctfmon.exe	3068	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
7:51:2...	ctfmon.exe	3068	RegOpenKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: R
7:51:2...	ctfmon.exe	3068	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
7:51:2...	ctfmon.exe	3068	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Desired Access: Q...
7:51:2...	ctfmon.exe	3068	RegQueryKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
7:51:2...	ctfmon.exe	3068	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Desired Access: Q...
7:51:2...	ctfmon.exe	3068	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	NAME NOT FOUND	Length: 144
7:51:2...	ctfmon.exe	3068	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
7:51:2...	ctfmon.exe	3068	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
7:51:2...	ctfmon.exe	3068	RegQueryValue	HKCU\Software\Microsoft\Input\Settin...	NAME NOT FOUND	Length: 144
7:51:2...	ctfmon.exe	3068	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Se...	SUCCESS	
7:51:2...	ctfmon.exe	3068	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
7:51:2...	ctfmon.exe	3068	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...

Showing 197,475 of 387,060 events (51%)      Backed by virtual memory

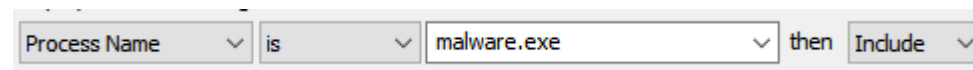
# Introducción al análisis dinámico

## Presentación de las herramientas – Process Monitor

Una de las mejores funcionalidades es la poner filtros en la captura de los eventos, de esta forma puedes filtrar para obtener los resultados asociados a la actividad que deseas.



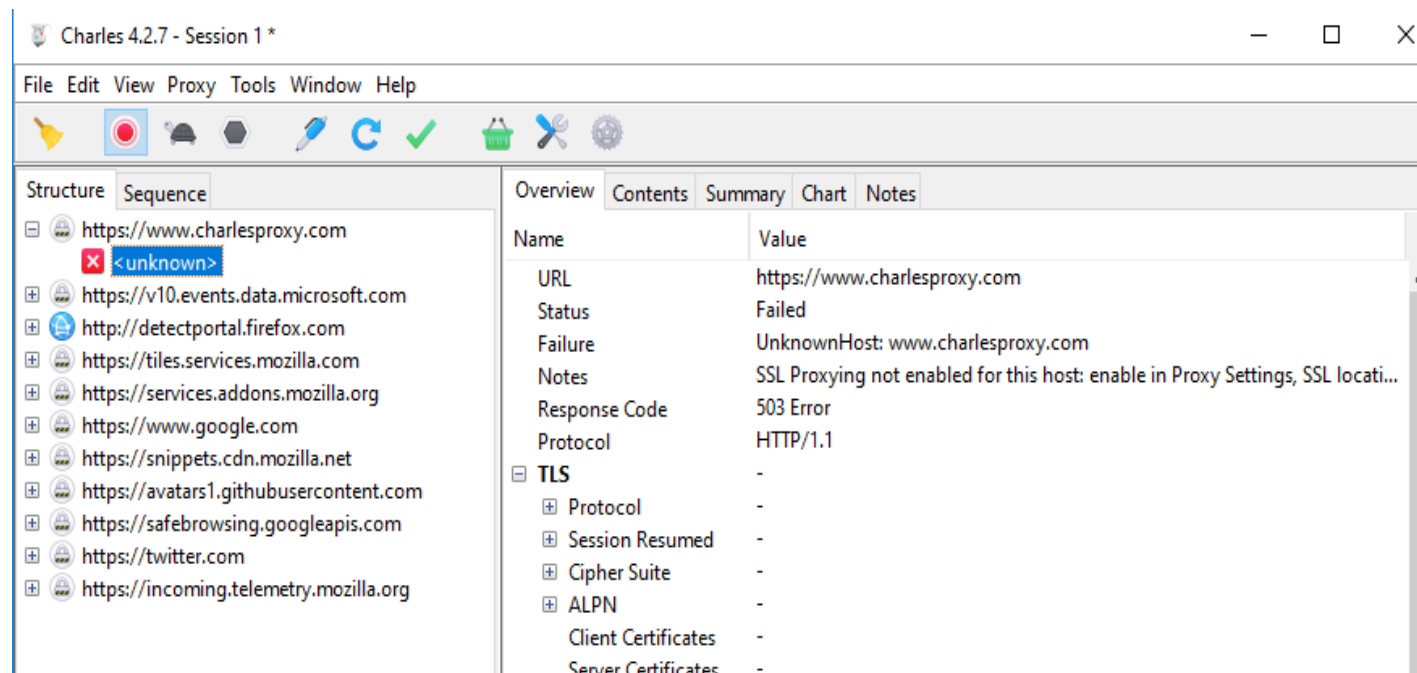
Filtro que muestra los eventos relativos al ejecutable malware.exe



# Introducción al análisis dinámico

## Presentación de las herramientas - Charles Proxy – Proxy de red

Esta herramienta es un HTTP proxy, con ella puedes obtener las conexiones HTTP que puede tener la sample.



# Introducción al análisis dinámico

## Presentación de las herramientas - Wireshark

Analizador de protocolos de red, permite ver todo el tráfico que pasa a través de una red.

2018-07-15-traffic-analysis-exercise.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Request - Transaction ID 0x20640255
2	0.005380	10.0.0.1	10.0.0.201	DHCP	342	DHCP ACK - Transaction ID 0x20640255
3	0.055967	10.0.0.201	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any sources
4	0.075418	10.0.0.201	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
5	0.081920	10.0.0.201	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
6	0.081920	10.0.0.201	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
7	0.082930	10.0.0.201	224.0.0.251	MDNS	80	Standard query 0x0000 ANY BLANCO-DESKTOP.local, "q?" question
8	0.083419	10.0.0.201	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.0.0.201
9	0.083420	10.0.0.201	224.0.0.252	LLMNR	74	Standard query 0x5fe2 ANY BLANCO-DESKTOP
10	0.189942	10.0.0.201	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any sources / Join group 224.0.0.252 for any sources
11	0.228954	10.0.0.201	10.0.0.2	DNS	97	Standard query 0x2428 SRV _ldap._tcp.dc._msdcs.dogoftheyear.net
12	0.228955	10.0.0.2	10.0.0.201	DNS	165	Standard query response 0x2428 SRV _ldap._tcp.dc._msdcs.dogoftheyear.net SRV 0 100 389 DogOfTheYear-DC.dogoftheyear.net A 10.0.0.2
13	0.233431	10.0.0.201	10.0.0.2	DNS	92	Standard query 0x55b1 A DogOfTheYear-DC.dogoftheyear.net
14	0.233431	10.0.0.2	10.0.0.201	DNS	108	Standard query response 0x55b1 A DogOfTheYear-DC.dogoftheyear.net A 10.0.0.2
15	0.243059	10.0.0.201	10.0.0.2	LDAP	266	searchRequest(1) "<root>" baseObject
16	0.243059	10.0.0.2	10.0.0.201	LDAP	244	searchResEntry(1) "<root>" searchResDone(1) success [1 result]
17	0.348376	10.0.0.201	10.0.0.2	TCP	66	49667 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	0.348377	10.0.0.2	10.0.0.201	TCP	66	389 → 49667 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	0.348377	10.0.0.201	10.0.0.2	TCP	54	49667 → 389 [ACK] Seq=1 Ack=1 Win=525568 Len=0
20	0.348377	10.0.0.201	10.0.0.2	LDAP	404	searchRequest(2) "<root>" baseObject
21	0.348466	10.0.0.2	10.0.0.201	TCP	1514	389 → 49667 [ACK] Seq=1 Ack=351 Win=525568 Len=1460 [TCP segment of a reassembled PDU]
22	0.348468	10.0.0.2	10.0.0.201	LDAP	1355	searchResEntry(2) "<root>"   searchResDone(2) success [1 result]
23	0.349005	10.0.0.201	10.0.0.2	TCP	54	49667 → 389 [ACK] Seq=351 Ack=2762 Win=525568 Len=0
24	0.361998	10.0.0.201	10.0.0.2	DNS	109	Standard query 0xc87e SRV _ldap._tcp.dc._msdcs.localdomain.dogoftheyear.net
25	0.361999	10.0.0.2	10.0.0.201	DNS	188	Standard query response 0xc87e No such name SRV _ldap._tcp.dc._msdcs.localdomain.dogoftheyear.net SOA dogoftheyear-dc.dogoftheyear.net
26	0.379201	10.0.0.201	10.0.0.2	DNS	76	Standard query 0xd8e8 A dns.msftncsi.com

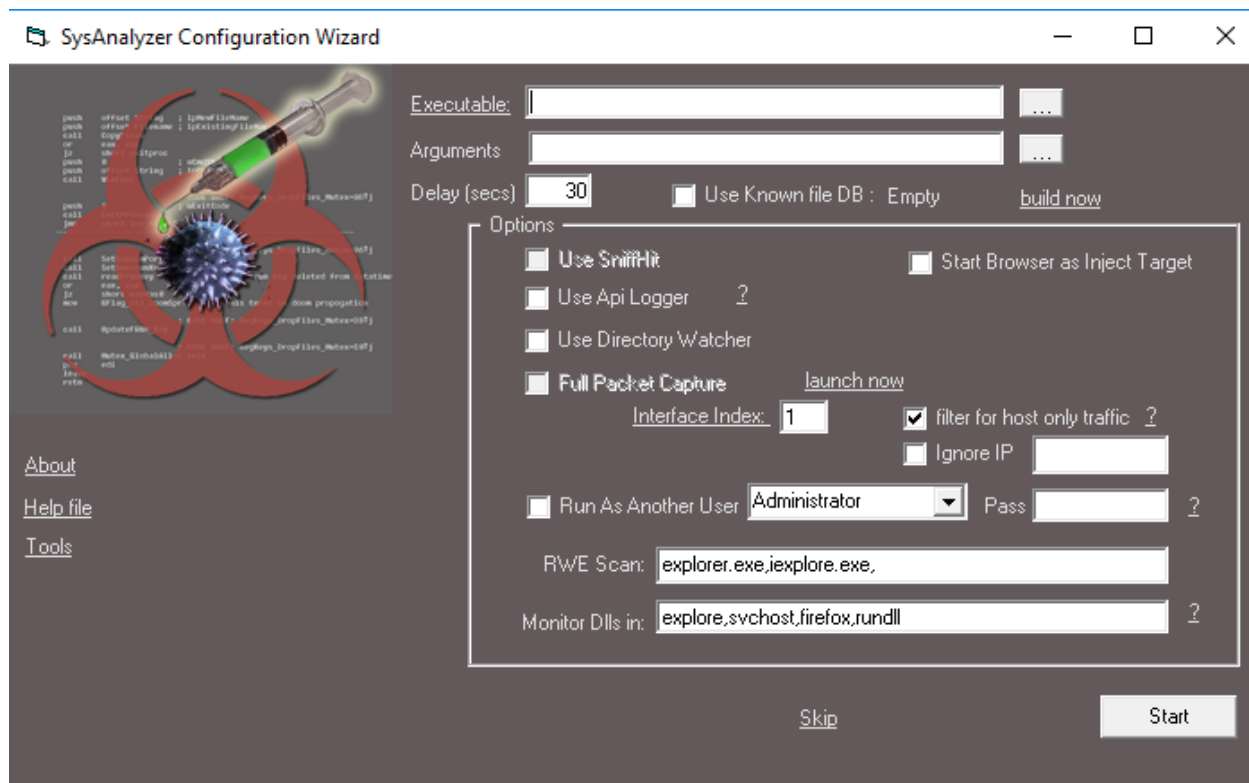
> Frame 1: 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits)  
> Ethernet II, Src: Msi\_18:66:c8 (00:16:17:18:66:c8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
> User Datagram Protocol, Src Port: 68, Dst Port: 67  
> Bootstrap Protocol (Request)

```
0000 ff ff ff ff ff ff 00 16 17 18 66 c8 00 00 45 00 .....f...E
0010 01 6d 4b 36 00 00 00 11 ee 4a 00 00 00 ff ff ...mK6...J....
0020 ff ff 00 44 00 43 01 59 4d d0 01 01 06 00 20 64 ...D-C-Y M....d
0030 02 55 00 00 00 00 00 00 00 00 00 00 00 00 00 ...U.....
0040 00 00 00 00 00 00 15 17 18 66 c3 00 00 00 00 .....f...
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0110 00 00 00 00 00 63 82 53 63 35 01 03 3d 07 01 ...c ScS...m...
0120 00 16 17 18 66 c8 32 04 0a 00 00 c9 0c 0e 42 4c ...f.2....BL
0130 41 4e 43 4f 2d 44 45 53 40 54 4f 50 51 22 00 00 ...ANCO-DES KTOPQ...
```

# Introducción al análisis dinámico

## Presentación de las herramientas - SysAnalyzer

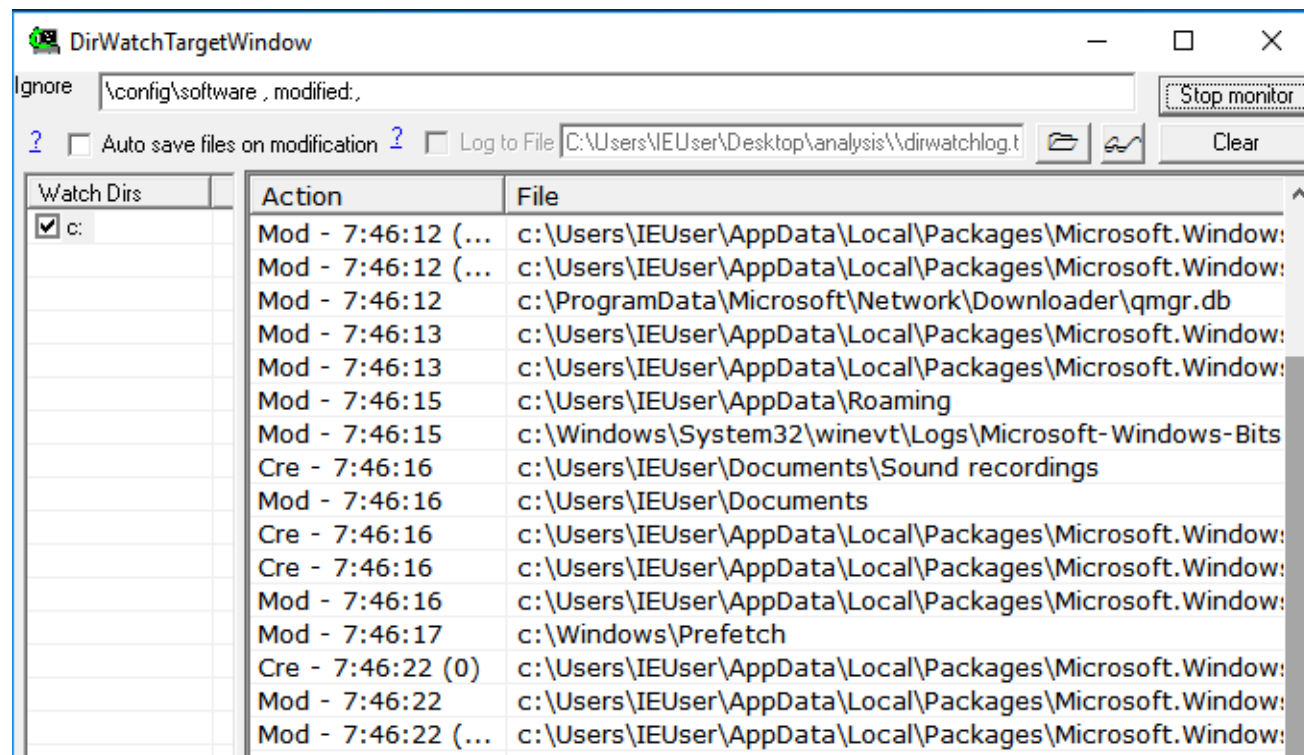
Esta herramienta permite la monitorización en tiempo real de la ejecución de una muestra, una vez finalizada la monitorización se obtiene un informe detallado con la recopilación de la información que ha obtenido en la ejecución.



# Introducción al análisis dinámico

## Presentación de las herramientas DirWatch

Esta utilidad pertenece a la Suite de SysAnalyzer permite la monitorización de una carpeta y captura los eventos de escritura/lectura en la carpeta.

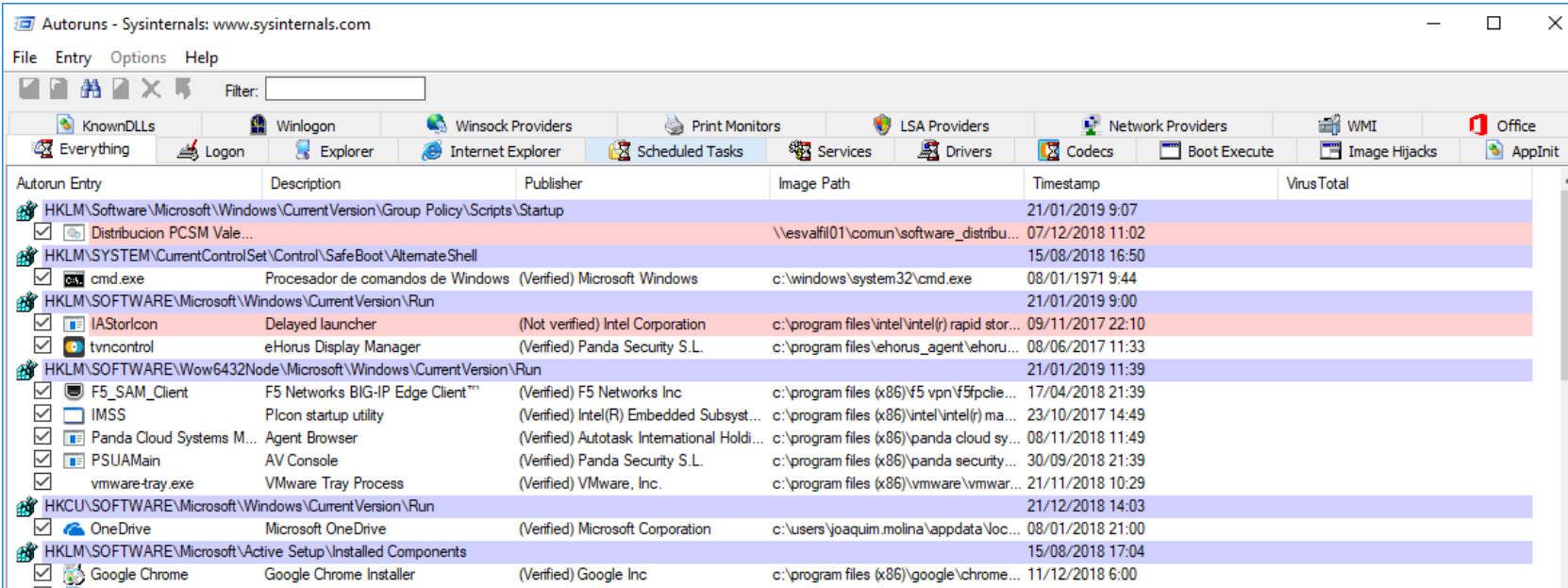


# Introducción al análisis dinámico

## Presentación de las herramientas Sysinternals Suite

Es un paquete de utilidades para realizar tareas de administración en los ordenadores Windows, contiene diferentes programas que te permiten analizar procesos, el disco, red, etc.

Una de las utilidades más utilizadas es Autoruns, que enumera la lista de todos los programas y procesos que se encuentran en el inicio del sistema.



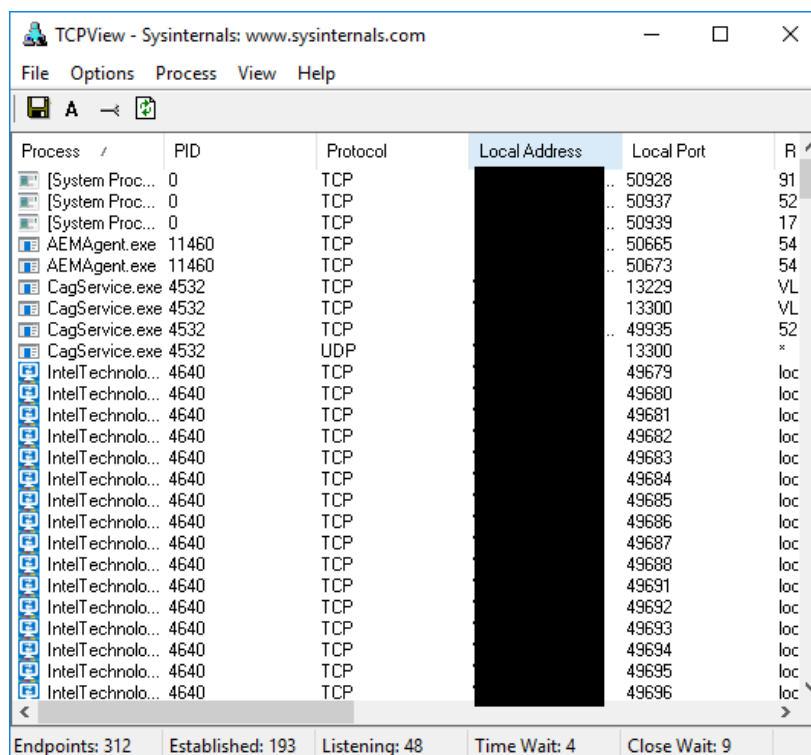
The screenshot shows the Autoruns application window. The title bar reads "Autoruns - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Entry", "Options", and "Help". Below the menu bar is a toolbar with icons for "Filter", "Logon", "Explorer", "Internet Explorer", "Scheduled Tasks", "Services", "Drivers", "Codecs", "Boot Execute", "Image Hijacks", and "AppInit". The main area is a table with columns: "Autorun Entry", "Description", "Publisher", "Image Path", "Timestamp", and "VirusTotal". The table lists various startup items, including system files like "cmd.exe" and "vmware-tray.exe", as well as third-party applications like "F5 Networks BIG-IP Edge Client" and "Google Chrome".

Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup				21/01/2019 9:07	
<input checked="" type="checkbox"/> Distribucion PCSM Vale...			\\esvalfi01\comun\software_distribu...	07/12/2018 11:02	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				15/08/2018 16:50	
<input checked="" type="checkbox"/> cmd.exe	Procesador de comandos de Windows	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	08/01/1971 9:44	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				21/01/2019 9:00	
<input checked="" type="checkbox"/> IAStorIcon	Delayed launcher	(Not verified) Intel Corporation	c:\program files\intel\intel(r) rapid stor...	09/11/2017 22:10	
<input checked="" type="checkbox"/> tvncontrol	eHorus Display Manager	(Verified) Panda Security S.L.	c:\program files\ehorus_agent\ehoru...	08/06/2017 11:33	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				21/01/2019 11:39	
<input checked="" type="checkbox"/> F5_SAM_Client	F5 Networks BIG-IP Edge Client™	(Verified) F5 Networks Inc	c:\program files (x86)\f5_vpn\Yf5fpclie...	17/04/2018 21:39	
<input checked="" type="checkbox"/> IMSS	PIcon startup utility	(Verified) Intel(R) Embedded Subsys...	c:\program files (x86)\intel\intel(r) ma...	23/10/2017 14:49	
<input checked="" type="checkbox"/> Panda Cloud Systems M...	Agent Browser	(Verified) Autotask International Holdi...	c:\program files (x86)\panda cloud sy...	08/11/2018 11:49	
<input checked="" type="checkbox"/> PSUAMain	AV Console	(Verified) Panda Security S.L.	c:\program files (x86)\panda security...	30/09/2018 21:39	
<input checked="" type="checkbox"/> vmware-tray.exe	VMware Tray Process	(Verified) VMware, Inc.	c:\program files (x86)\vmware\vmwar...	21/11/2018 10:29	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				21/12/2018 14:03	
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	c:\users\joaquim.molina\AppData\Loc...	08/01/2018 21:00	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				15/08/2018 17:04	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google Inc	c:\program files (x86)\google\chrome...	11/12/2018 6:00	

# Introducción al análisis dinámico

## Presentación de las herramientas Sysinternals Suite

Con la utilidad TcpView puedes ver las conexiones TCP/UDP que se encuentran activas en el ordenador en ese momento, útil para determinar conexiones persistentes con servidores externos.



The screenshot shows the TCPView application window with the following data:

Process	PID	Protocol	Local Address	Local Port	R
[System Proc...	0	TCP	..	50928	91
[System Proc...	0	TCP	..	50937	52
[System Proc...	0	TCP	..	50939	17
AEMAgent.exe	11460	TCP	..	50665	54
AEMAgent.exe	11460	TCP	..	50673	54
CagService.exe	4532	TCP	..	13229	VL
CagService.exe	4532	TCP	..	13300	VL
CagService.exe	4532	TCP	..	49935	52
CagService.exe	4532	UDP	..	13300	*
IntelTechnolo...	4640	TCP	..	49679	loc
IntelTechnolo...	4640	TCP	..	49680	loc
IntelTechnolo...	4640	TCP	..	49681	loc
IntelTechnolo...	4640	TCP	..	49682	loc
IntelTechnolo...	4640	TCP	..	49683	loc
IntelTechnolo...	4640	TCP	..	49684	loc
IntelTechnolo...	4640	TCP	..	49685	loc
IntelTechnolo...	4640	TCP	..	49686	loc
IntelTechnolo...	4640	TCP	..	49687	loc
IntelTechnolo...	4640	TCP	..	49688	loc
IntelTechnolo...	4640	TCP	..	49691	loc
IntelTechnolo...	4640	TCP	..	49692	loc
IntelTechnolo...	4640	TCP	..	49693	loc
IntelTechnolo...	4640	TCP	..	49694	loc
IntelTechnolo...	4640	TCP	..	49695	loc
IntelTechnolo...	4640	TCP	..	49696	loc

Summary statistics at the bottom of the window:

Endpoints: 312	Established: 193	Listening: 48	Time Wait: 4	Close Wait: 9
----------------	------------------	---------------	--------------	---------------

---

# ¡Manos a la obra!

**Objetivo: conseguir la mayor información posible sobre la amenaza.**

El departamento de soporte ha detectado una amenaza de malware en diversos equipos corporativos dentro de la red de un cliente, a continuación nos envían al laboratorio las siguientes muestras.

Vuestro trabajo es descubrir que acciones realiza y obtener la mayor cantidad de información posible.



---

# Bibliografía

## Documentación

1. **Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software.** [Michael Sikorski](#), [Andrew Honig](#)
2. **Learning Malware Analysis.** Monnapa K.A.
3. **MSDN, Documentación de la API de Windows** <https://docs.microsoft.com/en-us/windows/desktop/index>

# Reinventing Cybersecurity.



[pandasecurity.com](https://pandasecurity.com)