## Ofuscación de malware

## Descripción de las herramientas necesarias para el análisis de malware

**PEstudio** 

X64dbg

Scylla

### Análisis estático de la prueba de malware descargada

La prueba de Malware descargada es una versión de Black Mo<br/>on detectada el  $03\mbox{-}12\mbox{-}2019$ 

Podemos ver en la siguiente captura de pantalla, pruebas de que el malware a analizar ha sido empaquetado por una herramienta bastante conocida llamada UPX

Otro indicativo de que el binario ha sido comprimido es que la diferencia entre el tamaño virtual y el tamaño real es enorme, tanto, que el tamaño real de la parte comprimida es 0.

Vemos ademas, como en las cabeceras opcionales nos dice que el Address of Entry Point es en UPXO

Todas estas indicaciones nos hacen concluir que se ha comprimido con UPX la sección UPX0, que, una vez ejecutado el malware, se iniciara la rutina de descompresión y se cederá el control a este sección, contenedora del malware, ya descomprimido.

#### Análisis dinámico del malware

Levantando la aplicación de Wireshark e INetSim para analizar el comportamiento del malware a nivel de red, vemos que hace una serie de peticiones al servidor DNS para averiguar las direcciones IP de lo que aparentemente, parece que sean los servidores C2.

Podemos ver que algunas de las direcciones que pide son:

- pxi.hognoob.se
- qia.hognoob.se
- · uio.hognoob.se
- uio.herohero.info

Al estar usando el INetSim, estas direcciones no se resuelven y el virus no es capaz de contactar con sus servidores C2.

En esta sección, se pretende encontrar alguna de las características estudiadas en el temario del curso.

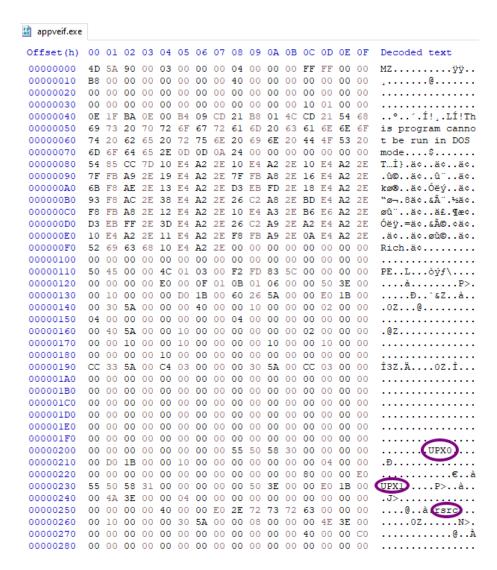


Figure 1: HxD prueba de UPX

Name	VirtualAd	VirtualSize	RawAddre	RawSize
UPX0	00001000	001BD000	00000400	00000000
UPX1	001BE000	003E5000	00000400	003E4A00
.rsrc	005A3000	00001000	003E4E00	00800000

Figure 2: PPEE Tamaño virtual vs raw

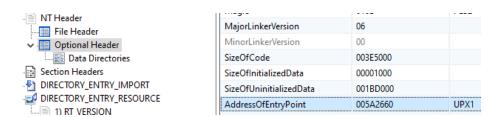


Figure 3: PPEE Address of Entry Point

```
Real start date : 2020-04-22 12:54:35
Simulated start date : 2020-04-22 12:54:35
Simulated start date : 2020-04-22 12:54:35
Simulated start date : 2020-04-22 12:54:35
2020-04-22 12:54:36
Bfts stimulated start date : 2020-04-22 12:54:35
2020-04-22 12:54:50
Bfts connection, type: A, class: IN, requested name: fp.msedge.net
1020-04-22 13:03:55
DMS connection, type: A, class: IN, requested name: fp.msedge.net
1020-04-22 13:03:55
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:29
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:29
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:29
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:29
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:29
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:29
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: A, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: sp.msedge.net
1020-04-22 13:23:23
DMS connection, type: PFR, class: IN, requested name: s
```

Figure 4: INetSim reporte filtrado

- Cifrado Cesar
- $\bullet$  Base64
- XOR
- identificación de cryptosignatures

# Análisis desde el punto de vista del empaquetado de ejecutables

En esta sección se pretende desempaquetar el malware seleccionado para posteriormente hacer un volcado de memoria virtual a disco y averiguar las cabeceras De esta forma, podemos analizar el malware como se ha creado desde el inicio, sin los inconvenientes introducidos por los packers.

Desempaquetado manual

Desempaquetado automático