incibe emprende

Programa de **Impulso a la Industria de la Ciberseguridad Nacional**

#**INCIBE**emprende

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

LOGOTIPO EMPRESA COLABORADORA

incibe emprende

INCIBE Emprende desarrolla iniciativas de **ideación, incubación y aceleración** tanto para la promoción del emprendimiento en ciberseguridad, como de la ciberseguridad en el emprendimiento de base tecnológica, con el fin de **Impulsar la Industria Nacional de Ciberseguridad**.

- **Acompañamos** a emprendedores y start-ups españolas de **ciberseguridad, así como de base tecnológica** para la integración de la ciberseguridad en su proyecto.
- **Impulsamos el desarrollo de proyectos** independientemente de su grado de madurez: fomento de ideas - incubación de proyectos - aceleración de start-ups e internacionalización.
- Impulsamos la **innovación** y promocionamos la atracción de **inversión** a la misma.

Plan de Recuperación, Transformación y Resiliencia (PRTR) a través del Componente 15. Inversión 7 Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, PYMES y profesionales e impulso del sector.

LOGOTIPO EMPRESA COLABORADORA

Start-ups vs emprendimiento tradicional

- Empresas digitales/base tecnológica
- Explotación de nuevos modelos de negocio
- Modelo de negocio escalable: crecimiento exponencial en ventas y crecimiento lineal en costes
- Ventaja competitiva basada en la innovación
- Alto riesgo debido a su alto contenido innovador
- Necesidad de elevado volumen de financiación y dificultad de acceso a la misma en fases iniciales
- Fuentes de financiación FFF (family, fools and Friends), capital riesgo, business angels. La garantía la supone el equipo.
- Dependencia en captación y retención de empleados altamente cualificados.

VS

- Explotación de modelos de negocio convencionales
- Crecimiento estable, modelo de negocio sostenible
- Fuente de financiación tradicional: préstamos y recursos propios. Garantía real y/o personal.
- Centrada en mantener el negocio y/o generar un crecimiento % estable.

LOGOTIPO EMPRESA COLABORADORA

Sector de la ciberseguridad

SECTOR EN AUGE

122.284
Trabajadores empleados (2021)

24.119
Brecha de talento (2021)

83.000
Brecha de talento (2024)

VALOR ECOSISTEMA*

1.500M
Año 2020

8,12%
Crecimiento anual

2.000M
Previsión 2024

*Fuente: Security Spending Guide IDC 2021

Participación mundial en la industria de ciberseguridad

31% 69%

Participación estudiantes grados STEM

24% 76%

Participación estudiantes cursos ciberseguridad

18% 82%

LOGOTIPO EMPRESA COLABORADORA

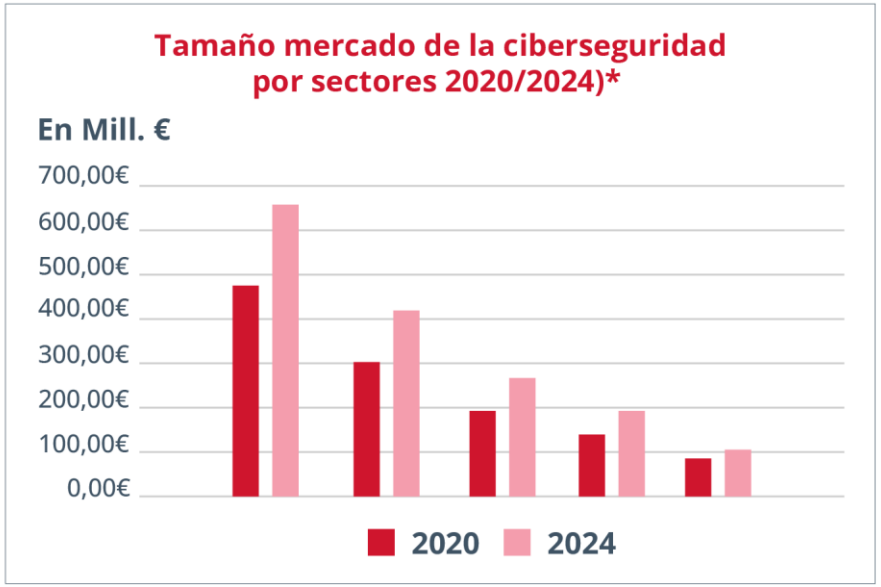
Sector de la ciberseguridad

Ciberseguridad

La importancia de la ciberseguridad es **transversal** a todos los sectores de la economía

Digitalización sectores

La digitalización de todos los sectores está favoreciendo un **crecimiento global del mercado de la Ciberseguridad**



El sector que más peso aporta a la ciberseguridad es el de **distribución y servicios**, seguido del **financiero**

*Fuente: Security Spending Guide IDC 2021

LOGOTIPO EMPRESA COLABORADORA

Programa de apoyo al Emprendimiento en ciberseguridad

incibe emprende 2023-2026

Captación / Ideación

Charlas
Talleres
Eventos

Incubación

Formación
Mentorización
Asesoramiento legal
Asesor fiscal
Visita al ecosistema regional
Demo Day

Aceleración

Formación
Mentorización
Asesoramiento legal
Asesor fiscal
Visita al ecosistema regional
Demo Day
Aceleración Express

LOGOTIPO EMPRESA COLABORADORA

Captación / Ideación

Título de la charla

- Presentación de la entidad
- Descripción de la charla

Las siguientes diapositivas serán las correspondientes al contenido de la charla correspondiente. En caso de querer añadir diapositivas, añadir una o duplicar la anterior.

Botón derecho > cambiar gráfico > escoger el logo de la entidad correspondiente

LOGOTIPO EMPRESA COLABORADORA

Desde las Profundidades del Kernel: Cómo Crear un Rootkit Invisible en WINDOWS

Descifrando el desarrollo de un Rootkit para Windows 11

INCIBE Emprende, 2025
[in/vazquez-vazquez-alejandro]

Whoami

- **FRIKI** (**F**anático de **R**evolucionar **I**nternamente **K**ernels e **I**nicios del sistema)

- Pastor de ovejas desde los 8 años
- Me gusta el pulpo, de ahí los Rootkits
- Docente en Máster de Análisis de Malware

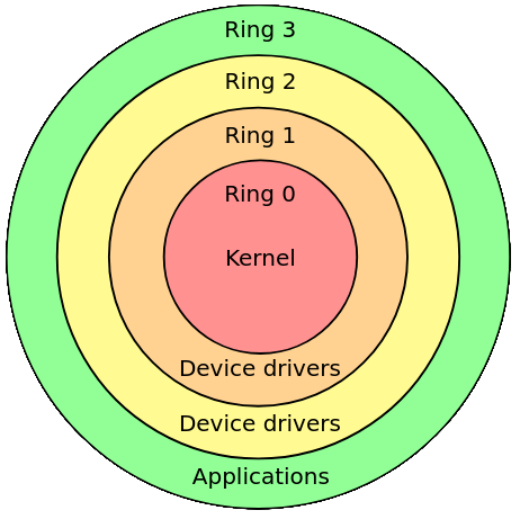
Table of Contents

Rootkit Development

Kernel (Ring 0)

The kernel (Ring 0) of an operating system implements the core functionality that everything else in the operating system depends upon. The Microsoft Windows kernel provides basic low-level operations such as scheduling threads or routing hardware interrupts. It is the heart of the operating system and all tasks it performs must be fast and simple.

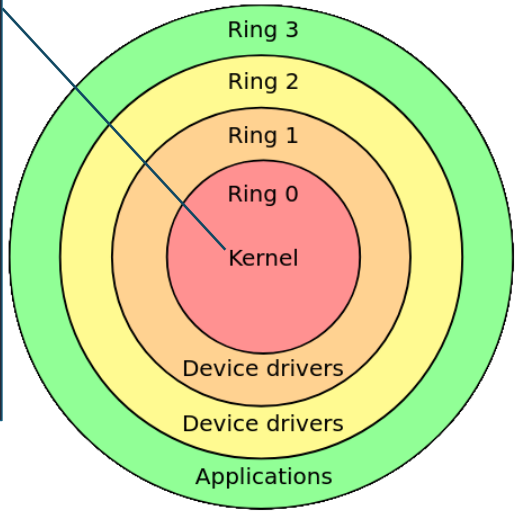
~ Microsoft



Kernel (Ring 0)

```
//0x150 bytes (sizeof)
struct _DRIVER_OBJECT
{
    SHORT Type;                                                          //0x0
    SHORT Size;                                                          //0x2
    struct _DEVICE_OBJECT* DeviceObject;                                 //0x8
    ULONG Flags;                                                         //0x10
    VOID* DriverStart;                                                   //0x18
    ULONG DriverSize;                                                    //0x20
    VOID* DriverSection;                                                 //0x28
    struct _DRIVER_EXTENSION* DriverExtension;                           //0x30
    struct _UNICODE_STRING DriverName;                                   //0x38
    struct _UNICODE_STRING* HardwareDatabase;                            //0x48
    struct _FAST_IO_DISPATCH* FastIoDispatch;                            //0x50
    LONG (*DriverInit)(struct _DRIVER_OBJECT* arg1, struct _UNICODE_STRING* arg2); //0x58
    VOID (*DriverStartIo)(struct _DEVICE_OBJECT* arg1, struct _IRP* arg2);  //0x60
    VOID (*DriverUnload)(struct _DRIVER_OBJECT* arg1);                   //0x68
    LONG (*MajorFunction[28])(struct _DEVICE_OBJECT* arg1, struct _IRP* arg2); //0x70
};
```

the core functionality that
e Microsoft Windows kernel
hreads or routing hardware
asks it performs must be fast



Rootkit

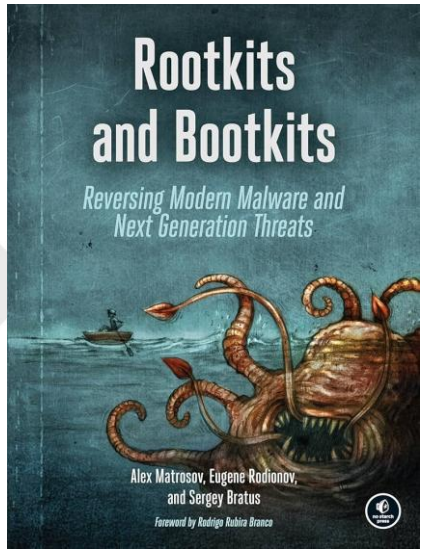
Rootkit: Sophisticated piece of malware that can add new code to the operating system or delete and edit operating system code. Rootkits may remain in place for years because they are hard to detect, due in part to their ability to block some antivirus software and malware scanner software.

~ Crowdstrike

Rootkit

Rootkit: Sophisticated piece of malware that can add new code to the operating system or delete and edit operating system code. Rootkits may remain in place for years because they are hard to detect, due in part to their ability to block some antivirus software and malware scanner software.

~ Crowdstrike



Kernel-Mode Driver → **C/C++ - driver.sys**

Security Mechanisms

[*Anti-Rootkit Installation*]

- Driver Signature Enforcement (DSE)

  Windows won't run drivers not certified by Microsoft

[*Anti-Rootkit Deep Funcionalities*]

- Kernel Patch Protection (PatchGuard)

  Feature of 64-bit editions of Microsoft Windows

  Prevents patching the kernel

Security Mechanisms

[*Anti-Rootkit Installation*]

- Driver Signature Enforcement (D

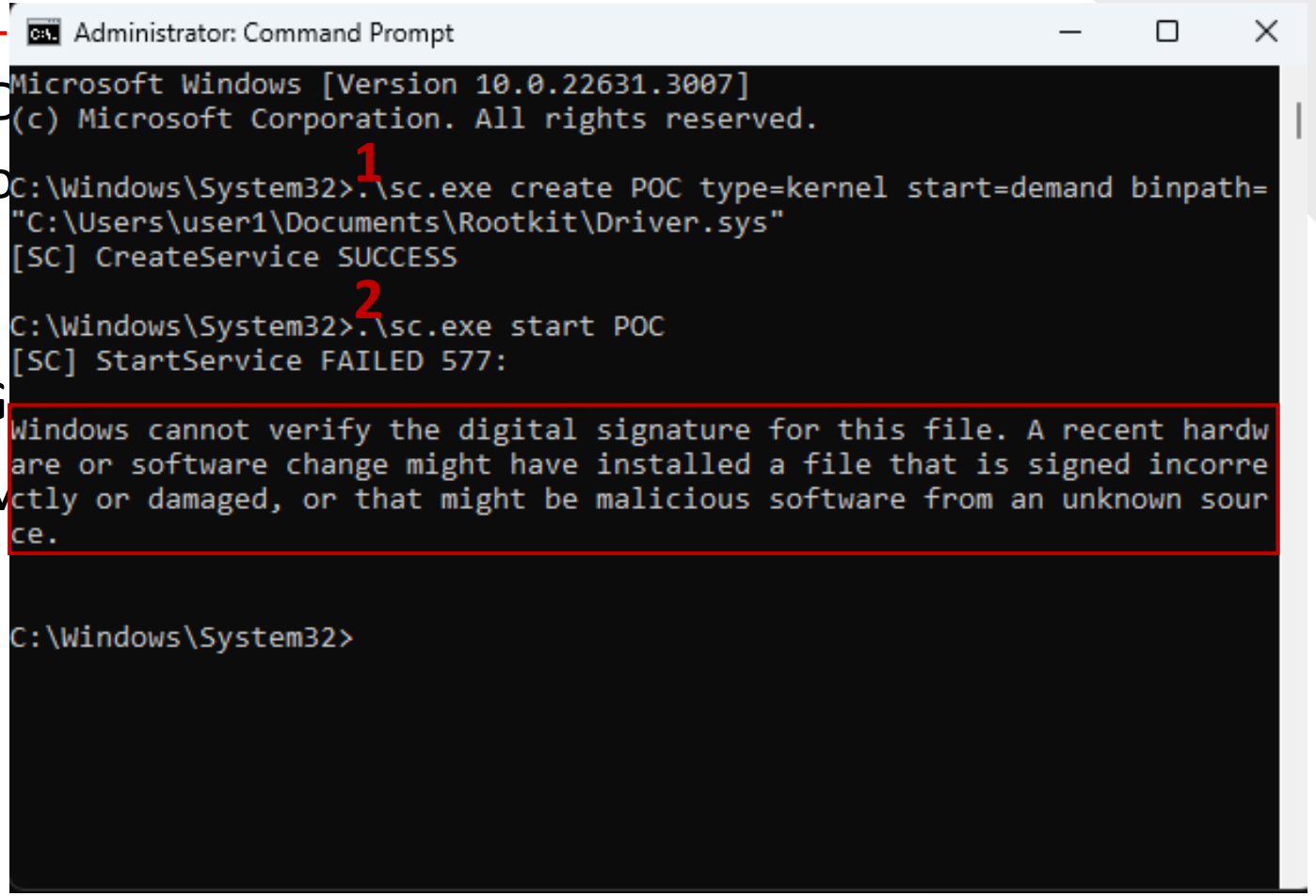
  Windows won't run drivers no

[*Anti-Rootkit Deep Funcionalities*]

- Kernel Patch Protection (PatchG

  Feature of 64-bit editions of M

  Prevents patching the kernel



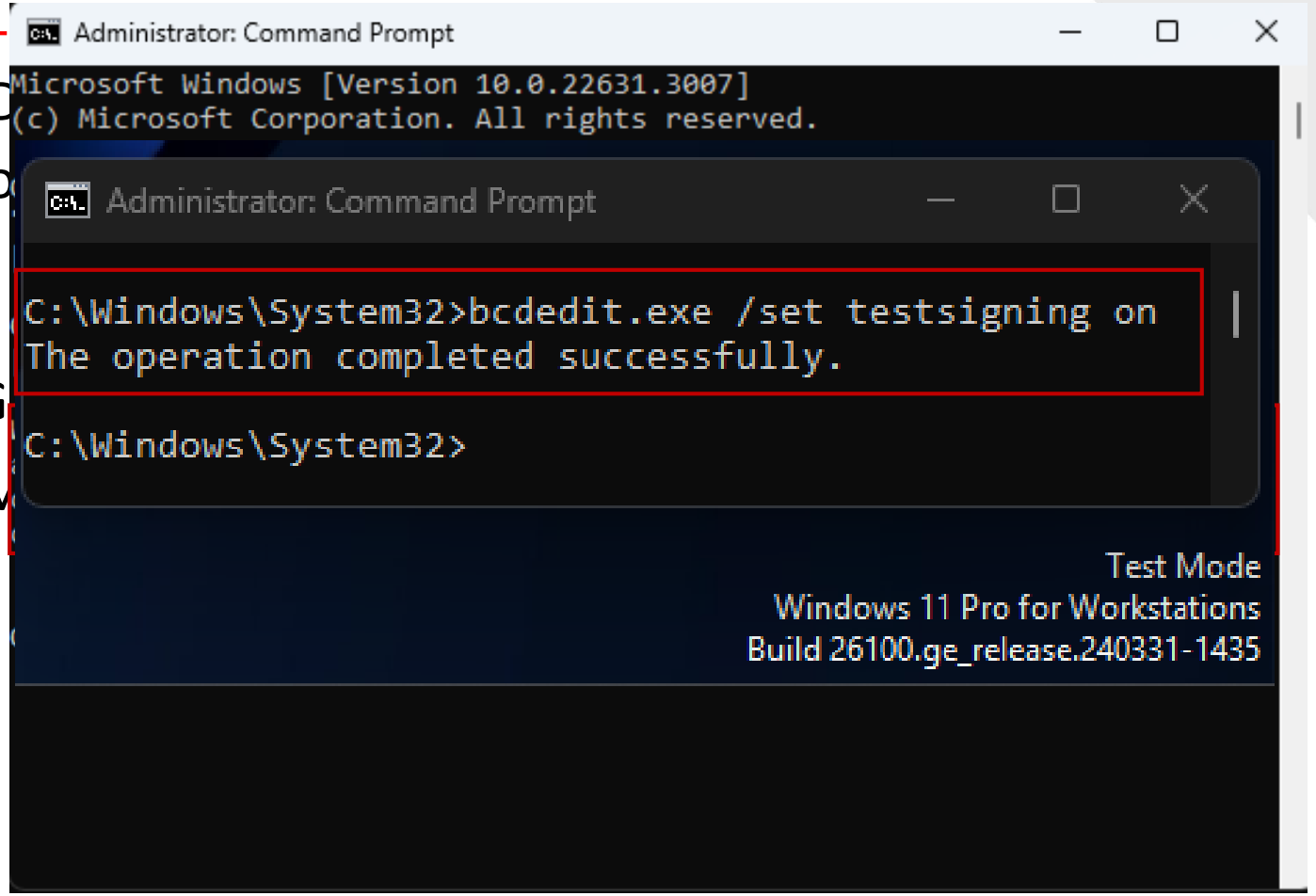
Security Mechanisms

[*Anti-Rootkit Installation*]

- Driver Signature Enforcement (D
  Windows won't run drivers no

[*Anti-Rootkit Deep Funcionalities*]

- Kernel Patch Protection (PatchG
  Feature of 64-bit editions of M
  Prevents patching the kernel



Security Mechanisms

[*Anti-Rootkit Installation*]

- Driver Signature Enforcement (D

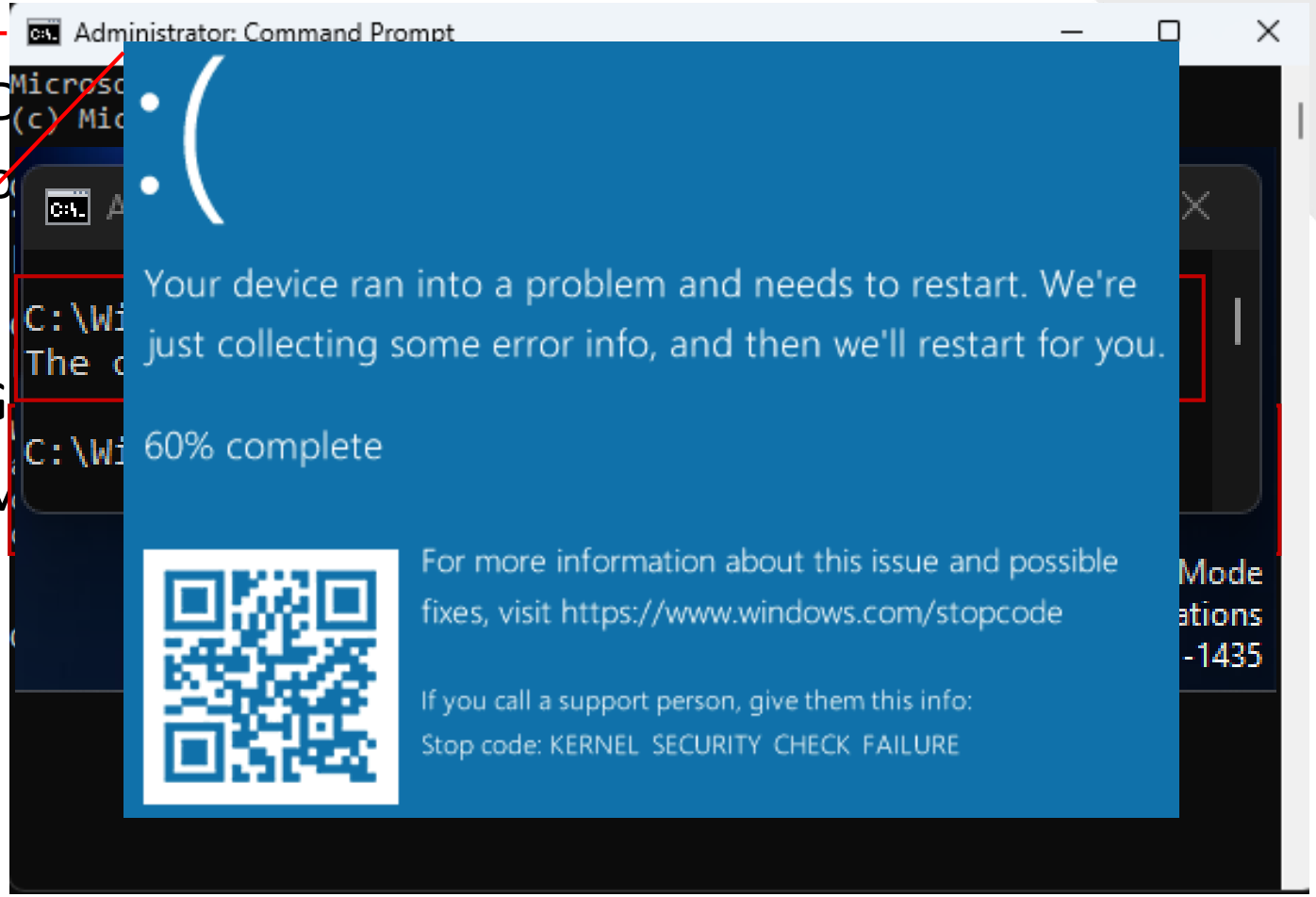
  Windows won't run drivers no

[*Anti-Rootkit Deep Funcionalities*]

- Kernel Patch Protection (PatchG

  Feature of 64-bit editions of M

  Prevents patching the kernel



Checkpoint

Rootkit Development

1. Windows Kernel
2. Rootkit = Kernel Mode Driver
3. DSE, PatchGuard, …

Development Environment

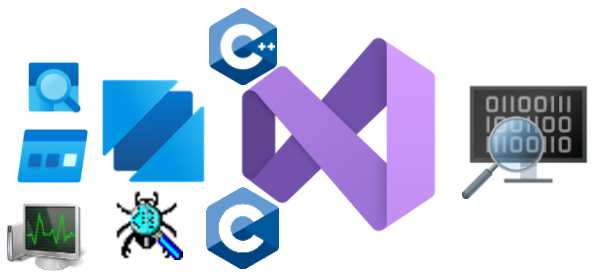
Learn / Windows / Windows Drivers /

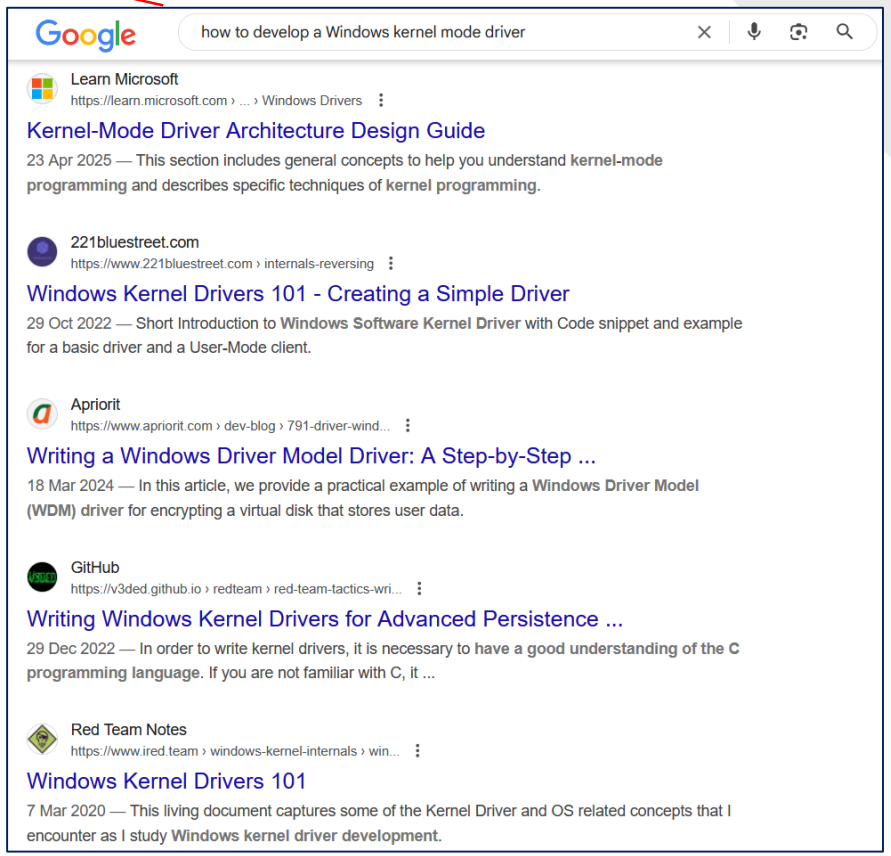
Tutorial: Write a Hello World Windows Driver (Kernel-Mode Driver Framework)

Article • 02/03/2025 • 10 contributors

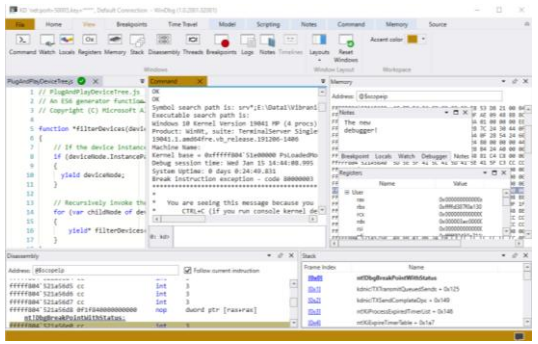
Feedback

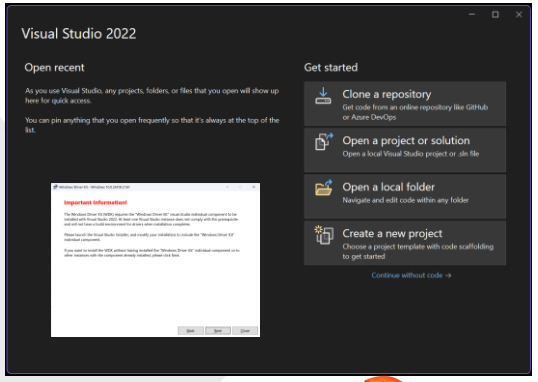
In this article

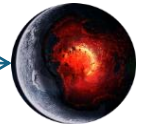


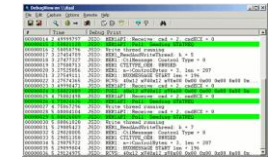


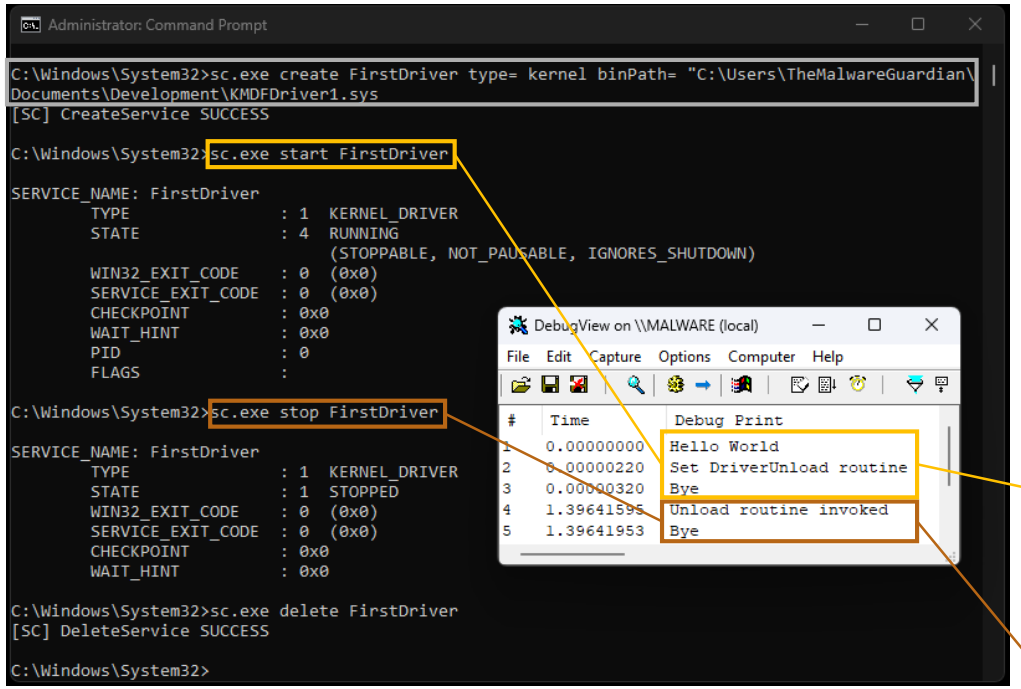
Development Environment

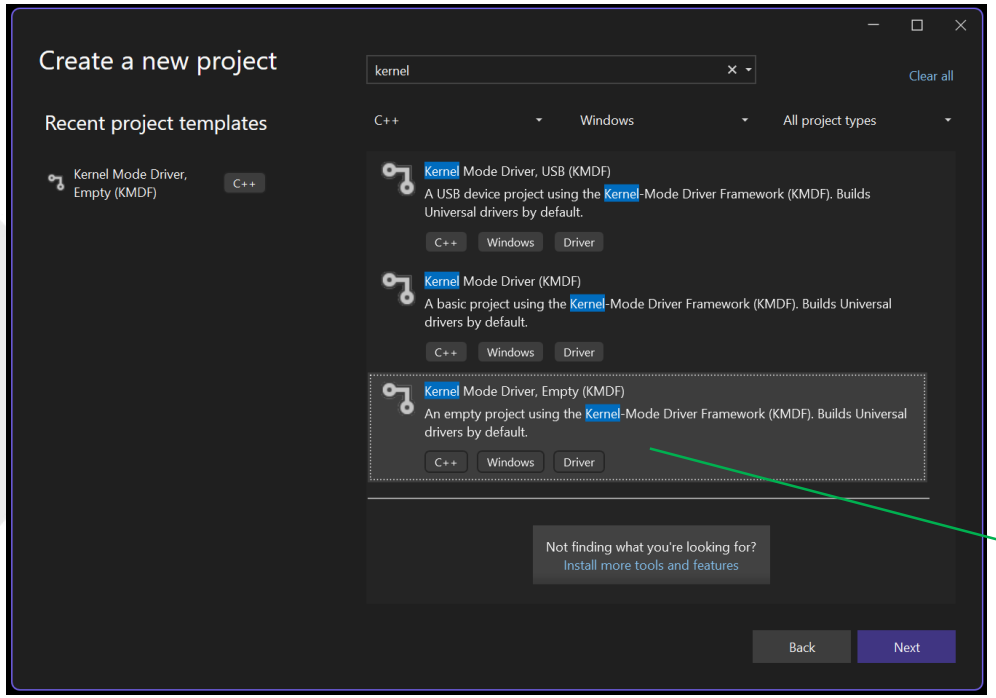


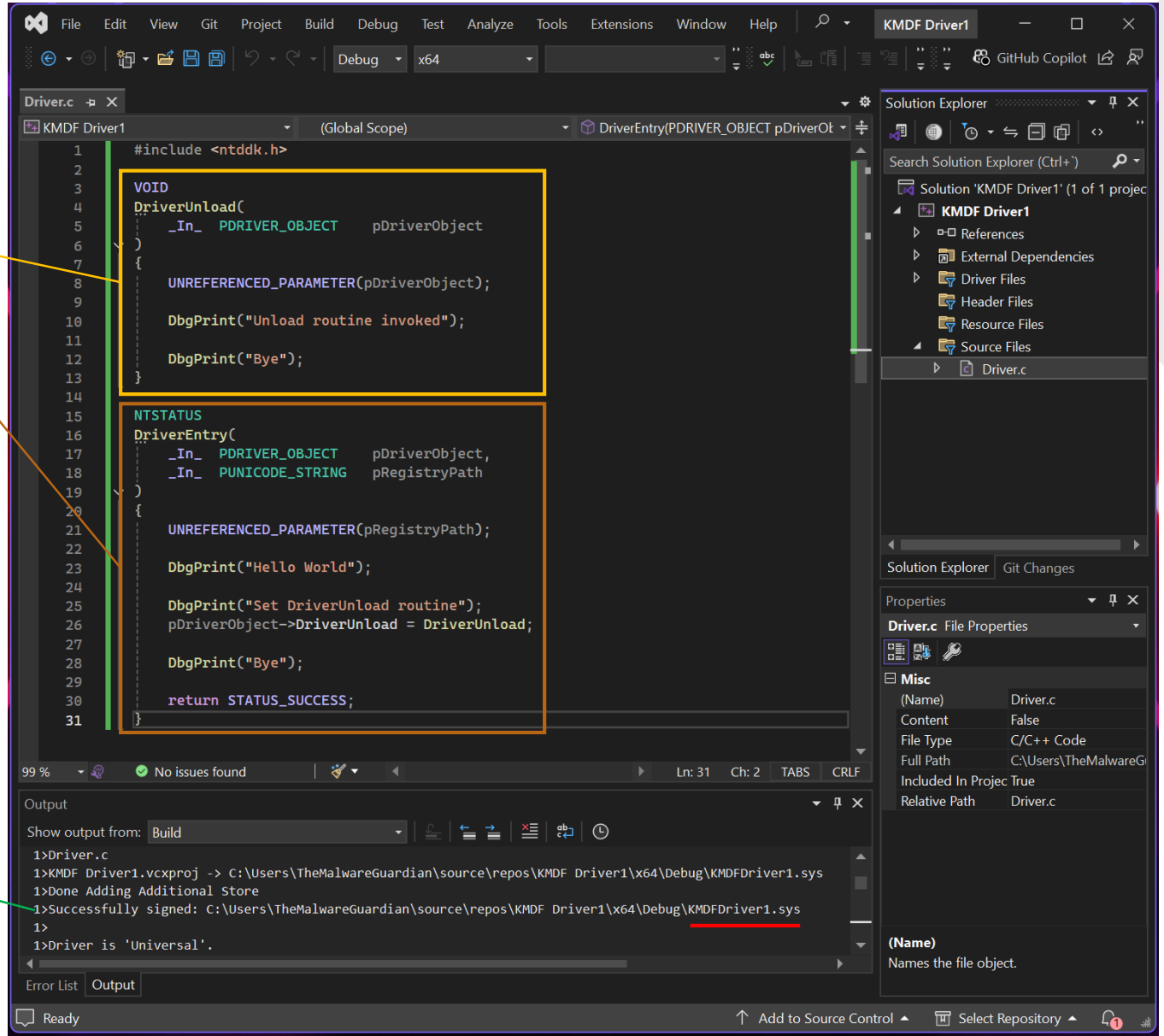







Administrator: Command Prompt
C:\Windows\System32>sc.exe create FirstDriver type= kernel binPath= "C:\Users\TheMalwareGuardian\Documents\Development\KMDFDriver1.sys
[SC] CreateService SUCCESS
C:\Windows\System32>sc.exe start FirstDriver
SERVICE_NAME: FirstDriver
TYPE : 1 KERNEL_DRIVER
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
PID : 0
FLAGS :
C:\Windows\System32>sc.exe stop FirstDriver
SERVICE_NAME: FirstDriver
TYPE : 1 KERNEL_DRIVER
STATE : 1 STOPPED
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
C:\Windows\System32>sc.exe delete FirstDriver
[SC] DeleteService SUCCESS
C:\Windows\System32>
DebugView on \\MALWARE (local)
File Edit Capture Options Computer Help
Time Debug Print
1 0.00000000 Hello World
2 0.00000220 Set DriverUnload routine
3 0.00000320 Bye
4 1.39641595 Unload routine invoked
5 1.39641953 Bye


Create a new project
kernel
Clear all
Recent project templates
Kernel Mode Driver, Empty (KMDF)
C++
C++
Windows
All project types
Kernel Mode Driver, USB (KMDF)
A USB device project using the Kernel-Mode Driver Framework (KMDF). Builds Universal drivers by default.
C++ Windows Driver
Kernel Mode Driver (KMDF)
A basic project using the Kernel-Mode Driver Framework (KMDF). Builds Universal drivers by default.
C++ Windows Driver
Kernel Mode Driver, Empty (KMDF)
An empty project using the Kernel-Mode Driver Framework (KMDF). Builds Universal drivers by default.
C++ Windows Driver
Not finding what you're looking for?
Install more tools and features
Back
Next


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
KMDF Driver1
Debug
x64
GitHub Copilot
Driver.c
KMDF Driver1
(Global Scope)
DriverEntry(PDRIVER_OBJECT pDriverOb
#include <ntddk.h>
VOID
DriverUnload(
_In_ PDRIVER_OBJECT pDriverObject
)
{
UNREFERENCED_PARAMETER(pDriverObject);
DbgPrint("Unload routine invoked");
DbgPrint("Bye");
}
NTSTATUS
DriverEntry(
_In_ PDRIVER_OBJECT pDriverObject,
_In_ PUNICODE_STRING pRegistryPath
)
{
UNREFERENCED_PARAMETER(pRegistryPath);
DbgPrint("Hello World");
DbgPrint("Set DriverUnload routine");
pDriverObject->DriverUnload = DriverUnload;
DbgPrint("Bye");
return STATUS_SUCCESS;
}
99 %
No issues found
Ln: 31 Ch: 2 TABS CRLF
Output
Show output from: Build
1>Driver.c
1>KMDF Driver1.vcxproj -> C:\Users\TheMalwareGuardian\source\repos\KMDF Driver1\x64\Debug\KMDFDriver1.sys
1>Done Adding Additional Store
1>Successfully signed: C:\Users\TheMalwareGuardian\source\repos\KMDF Driver1\x64\Debug\KMDFDriver1.sys
1>
1>Driver is 'Universal'.
Error List Output
Ready
Add to Source Control
Select Repository
Solution Explorer
Search Solution Explorer (Ctrl+;)
Solution 'KMDF Driver1' (1 of 1 projec
KMDF Driver1
References
External Dependencies
Driver Files
Header Files
Resource Files
Source Files
Driver.c
Solution Explorer Git Changes
Properties
Driver.c File Properties
Misc
(Name) Driver.c
Content False
File Type C/C++ Code
Full Path C:\Users\TheMalwareG
Included In Projec True
Relative Path Driver.c
(Name)
Names the file object.

Malicious Driver

1. User Mode - Kernel Mode Communication ntddk.h		Toolkit Communication
2. Direct Kernel Object Modification ntddk.h		Hide Processes DKOM
3. Keyboard and Mouse Filter ntddk.h		Keylogger Keyboard Filter
4. Windows Filtering Platform fwpmk.h, fwpsk.h, fwpmu.h		Network Control WFP
5. Windows Kernel Sockets wsk.h		Network Requests WSK
6. File System Minifilter Driver fltKernel.h		Hide Folders Minifilter

Bentico

KernelRootkit001_HelloWorld

KernelRootkit002_Threading

KernelRootkit003_ZwFunctions

KernelRootkit004_Callbacks

KernelRootkit005_IOCTLs

KernelRootkit006_DKOM

KernelRootkit007_KeyboardFilter

KernelRootkit008_Minifilter

KernelRootkit009_FilterCommunicationPort

KernelRootkit010_WindowsFilteringPlatform

KernelRootkit011_WinSockKernel

Communication

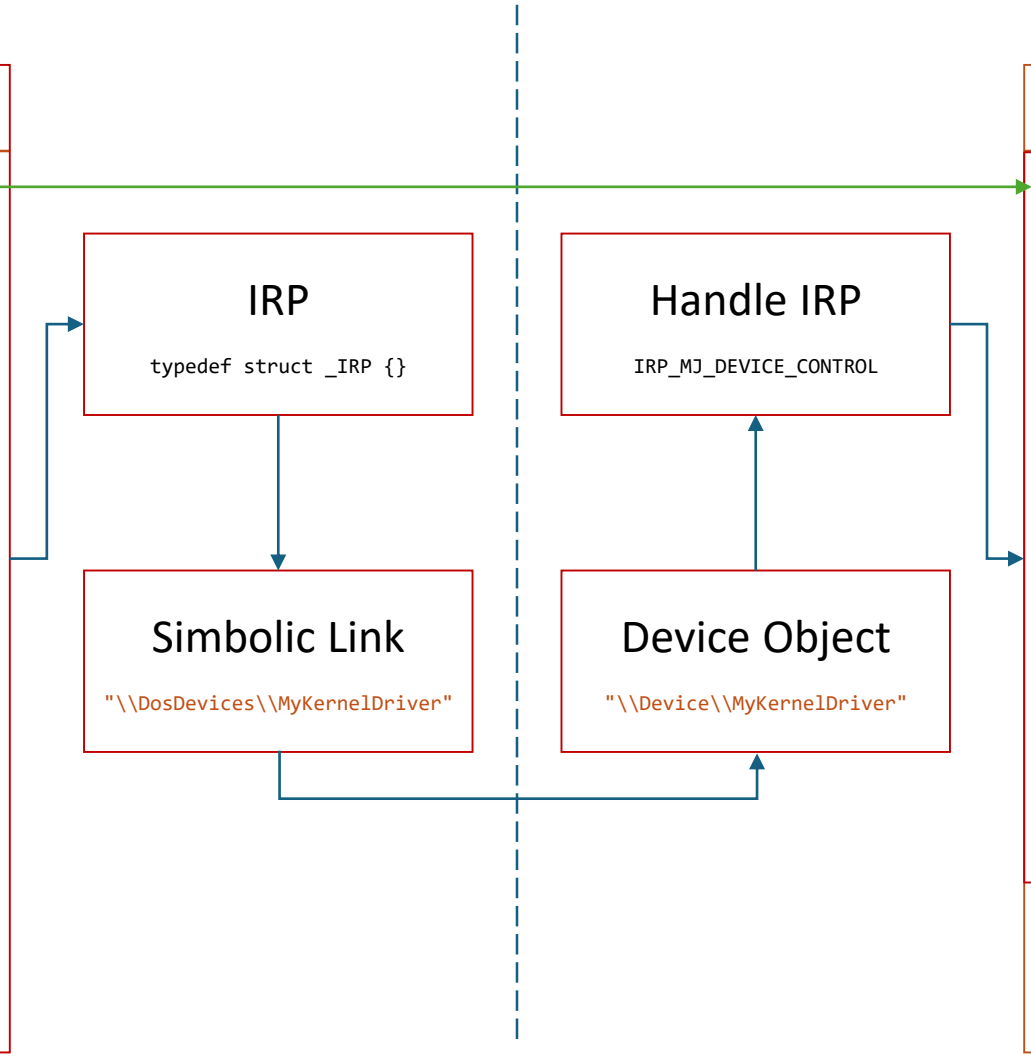
"The bridge between user mode and kernel mode:
IOCTL requests initiate communication, while IRPs manage data exchange and driver actions."

- ✓ Via Input/Output Control Codes and Input/Output Request Packets
- ✓ Via Filter Communication Ports
- ✗ Via Network Requests
- ✗ Via Shared Memory
- ✗ Via Registry Keys
- ✗ Via Files
- ✗ Via …

Communication

console_application.exe

```
// ------------------------
#define IOCTL_COMM_0 CTL_CODE(FILE_DEVICE_UNKNOWN, 0x800, METHOD_BUFFERED, FILE_ANY_ACCESS)


// ------------------------
hDevice = CreateFile(L"\\\\.\\MyKernelDriver", GENERIC_READ | GENERIC_WRITE, ...


// ------------------------
BOOL success = DeviceIoControl(hDevice,
                               1 IOCTL_COMM_0,
                               2 inBuffer, sizeof(inBuffer),
                               3 outBuffer, sizeof(outBuffer),
                               &bytesReturned, NULL);
```

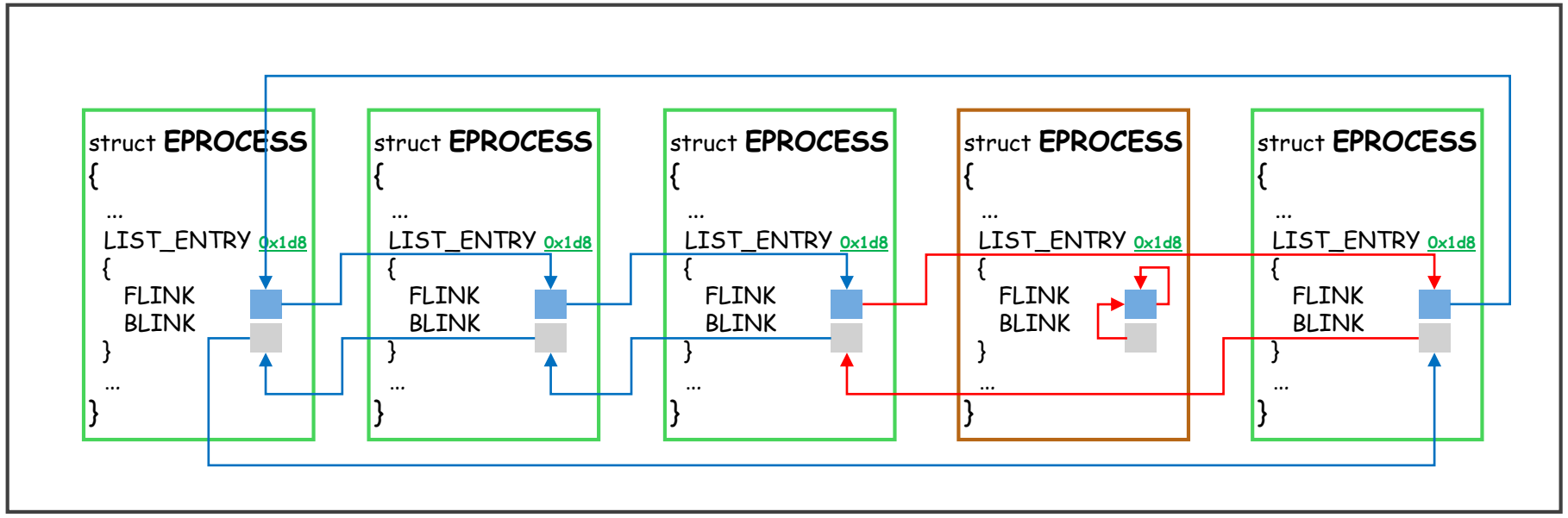


kernel_mode_driver.sys

```
// ------------------------
#define IOCTL_COMM_0 CTL_CODE(FILE_DEVICE_UNKNOWN, 0x800, METHOD_BUFFERED, FILE_ANY_ACCESS)


// ------------------------

status = IoCreateDevice(...);
status = IoCreateSymbolicLink(...);


// ------------------------
pDriverObject->MajorFunction[...] = ...;
pDriverObject->MajorFunction[IRP_MJ_DEVICE_CONTROL] = DriverHandleIOCTLs;


// ------------------------
NTSTATUS
DriverHandleIOCTLs(
    _In_  PDEVICE_OBJECT  pDeviceObject,
    _In_  PIRP            pIrp
)
{
    PIO_STACK_LOCATION stack = IoGetCurrentIrpStackLocation(pIrp);

    ULONG controlCode = stack->Parameters.DeviceIoControl.IoControlCode;

    switch (controlCode)
    {

        case IOCTL_COMM_0:
            ...
            break;

        case IOCTL_COMM_1:
            ...
            break;

    pIrp->IoStatus.Status = STATUS_SUCCESS;

    IoCompleteRequest(pIrp, IO_NO_INCREMENT);

    return STATUS_SUCCESS;
}
```

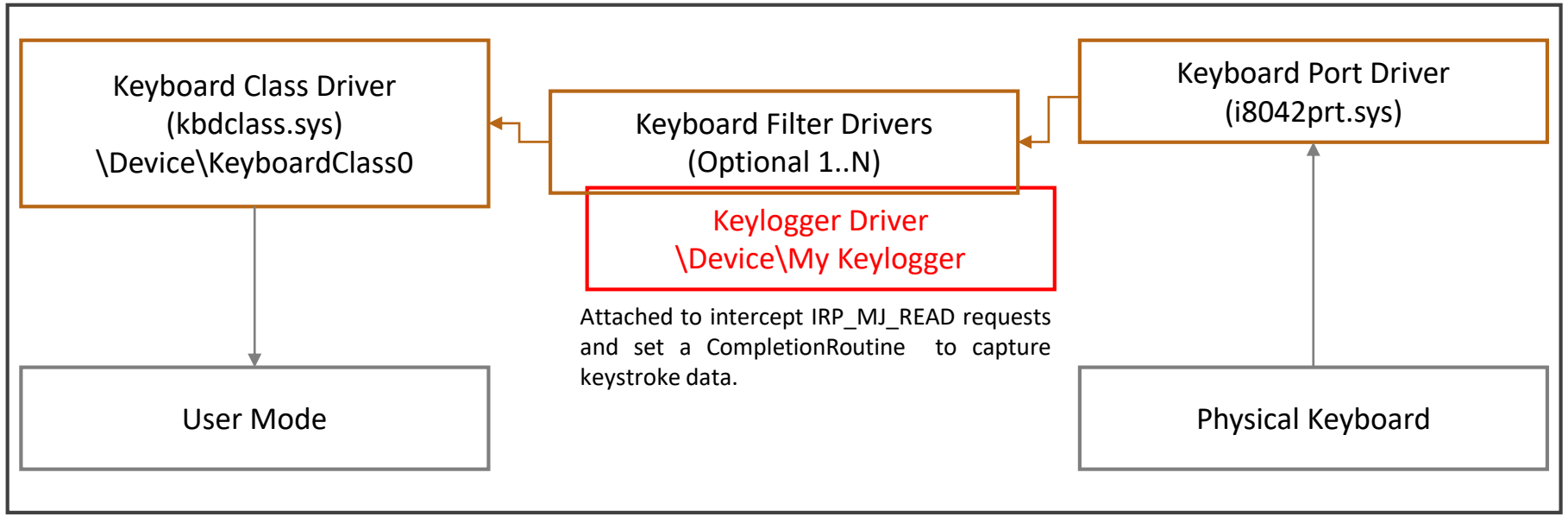
Hide Procesess

"Windows maintains a doubly linked list of active processes in (LIST_ENTRY) EPROCESS->ActiveProcessLinks. Unlink a process from the chain, and it disappears from user-mode enumeration."



Keylogger

"Keystroke interception in kernel mode: The Windows keyboard driver stack routes all keystrokes through a device object called \Device\KeyboardClass0. By attaching a driver to this device and registering a CompletionRoutine (a callback executed after an IRP has been processed by lower drivers, allowing access to data before it reaches the next stage), we can capture raw keystroke data before it propagates to user-mode applications like text editors or browsers."



The Gateway

Rootkit Installation

Kernel Mode Driver

The Gateway

1. Vulnerable Kernel Driver

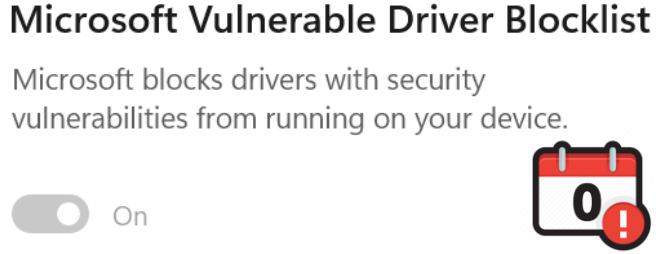
Rootkit Installation

Kernel Mode Driver

(BYOVD)

Bring Your Own Vulnerable Driver

Not Well Known



The Gateway

Rootkit Installation

Kernel Mode Driver

1. Vulnerable Kernel Driver

(BYOVD)
Bring Your Own Vulnerable Driver

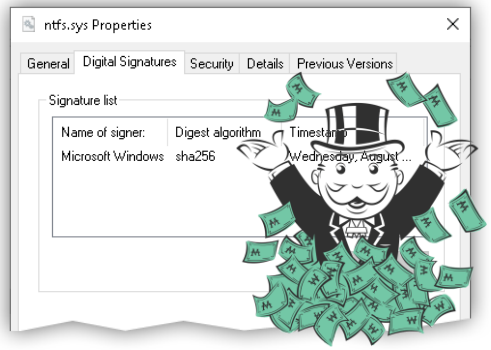
Not Well Known

2. Leaked Certificate

Driver Signing Policy

Microsoft Vulnerable Driver Blocklist

Microsoft blocks drivers with security vulnerabilities from running on your device.



The Gateway

Rootkit Installation

Kernel Mode Driver

1. Vulnerable Kernel Driver

(BYOVD)
Not Well Known
Bring Your Own Vulnerable Driver

2. Leaked Certificate

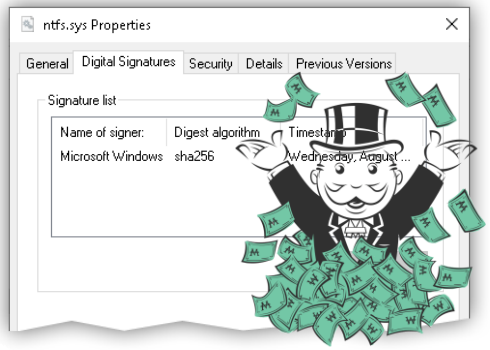
Driver Signing Policy

3. UEFI Bootkit

SecureBoot
Infect a Computer's Boot process
Physical Access

Microsoft Vulnerable Driver Blocklist

Microsoft blocks drivers with security vulnerabilities from running on your device.



B/Rootkits In The Wild

2022

MoonBounce

CosmicStrand

Fire Chili

2

2024

Bootkitty

Fudmodule

1

2021

ESPecter

3

FinSpy

Moriya

2023

BlackLotus

Fudmodule, Fire Chili, ESPecter

ESET Research

UEFI threats moving to the ESP: Introducing ESPecter bootkit

ESET research discovers a previously undocumented UEFI bootkit with roots going back all the way to at least 2012


Martin Smolár


Anton Cherepanov

05 Oct 2021 , 20 min. read


DEMO
LOADING...

Reverse Engineering / Malware Analysis / Bug Hunting

Module 10 – Windows Reverse Engineering

- Windows architecture (User mode and Kernel mode)
- Windows protections (DSE, KPP, VBS, CFG)
- Malware hunting with SysInternals tools
- Windows kernel opaque structures (EPROCESS, ETHREAD)
- Windows kernel debugging
- WinDbg scripting (Commands, Javascript, PyKd)
- Rootkit hooking techniques (IDT, SSDT)
- Rootkit development (Kernel Mode Drivers)
- Bootkit development (UEFI Applications)
- Bootkit analysis (ESPecter, BlackLotus)
- Kernel exploitation (Vulnerable drivers, Write-What-Where)

Thank You ☺

Every resource you need to develop Rootkits:

github.com/TheMalwareGuardian/Awesome-Bootkits-Rootkits-Development

Automate Bootkits/Rootkits Development

github.com/TheMalwareGuardian/Bootkits-Rootkits-Development-Environment

Contact:

www.linkedin.com/in/vazquez-vazquez-alejandro

¡Ahora te toca!

¿Tienes una idea de negocio en ciberseguridad, tu proyecto necesita de ciberseguridad?

¡Te ayudamos a emprender!

¡Apúntate a los próximos **talleres de emprendimiento**!

¡O solicita plaza en el programa de **Incubación de INCIBE Emprende**!

LOGOTIPO EMPRESA COLABORADORA

Ediciones anteriores

LOGOTIPO EMPRESA COLABORADORA

INCIBE Emprende

¡Te estamos esperando!

Indicar correo electrónico aquí

Indicar teléfono de contacto aquí

Indicar web aquí

incibe emprende

Programa de **Impulso a la Industria de la Ciberseguridad Nacional**

#INCIBEemprende

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

LOGOTIPO EMPRESA COLABORADORA