

<!--418-->

Desarrollo de  
malware pt.1{

<Que="es un compilador"/>

}



# Fases del desarrollo de malware {

01

Objetivo

02

Codigo  
fuente

03

Obfuscacion  
de codigo y  
anti-  
debugging

04

Inyeccion en  
procesos

05

Persistencia

06

Command and  
control

07

CLEANUP

}

PERO EN QUE LENGUAJEEEEEE {



PYTHON

FACIL DE PROGRAMAR  
ULTRA LENTO  
ULTRA DETECTABLE  
ULTRA PORTABLE



C#

MAS DIFICIL DE  
PROGRAMAR  
LIGERAMENTE MAS  
RAPIDO QUE PYTHON  
MENOS DETECTABLE  
MENOS PORTABLE



C/C++

DIFICIL DE  
PROGRAMAR  
ULTRA RAPIDO  
ULTRA  
PORTABLE  
DIFICIL DE  
DETECTAR

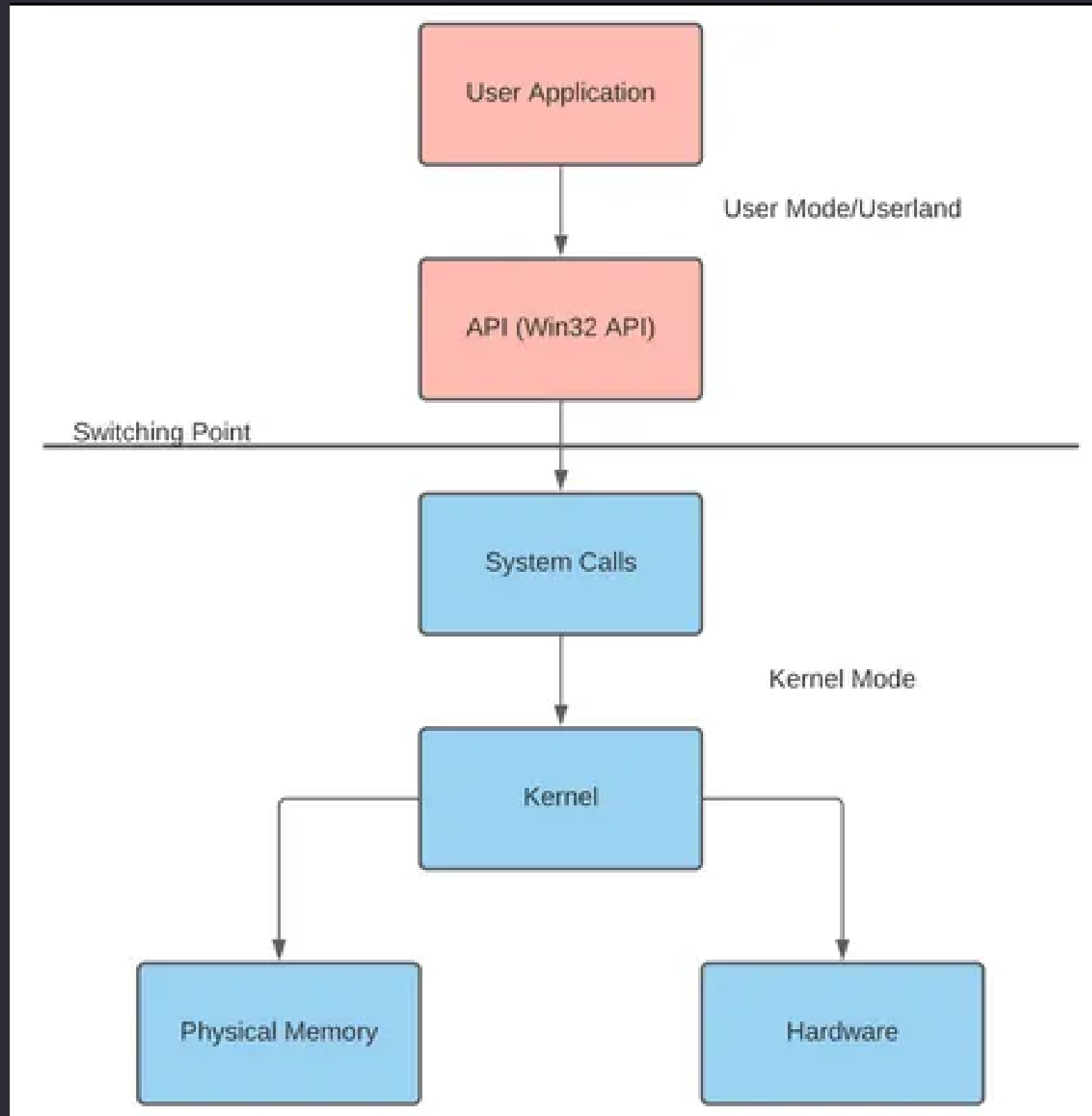


ASSEMBLY

EL MENOS  
DETECTABLE  
EL MAS RAPIDO  
EL MAS  
PORTABLE  
EL MAS  
DIFICIL DE  
PROGRAMAR

}

# Windows API {



Conjunto de aplicaciones y sistemas que permitena desarrolladores manipular los siguientes aspectos.

- Procesos y su memoria
- Registro de windows
- Redes
- Servicios
- Hooks

}

# Procesos y memoria

Dentro de todos los sistemas operativos existe un administrador de memoria. Este se encarga de llevar una gestión de la memoria asignada y libre.

Un proceso es una instancia de un programa que corre en memoria. Tiene un rango de memoria y un id de procesos PID.

La API de windows nos deja abrir procesos y editar su memoria a voluntad.

<https://learn.microsoft.com/en-us/windows/win32/procthread/process-and-thread-functions>

0000 0000 0000 0000	0000	
0000 0000 0000 0001	0001	
0000 0000 0000 0010	0002	
0000 0000 0000 0011	0003	
0000 0000 0000 0100	0004	
0000 0000 0000 0101	0005	
		...
0000 0000 0100 1001	0049	
0000 0000 0100 1010	004A	
0000 0000 0100 1011	004B	
		...
1111 1111 1111 1111	FFFF	
Binary	Hex	Memory
Address		Bytes

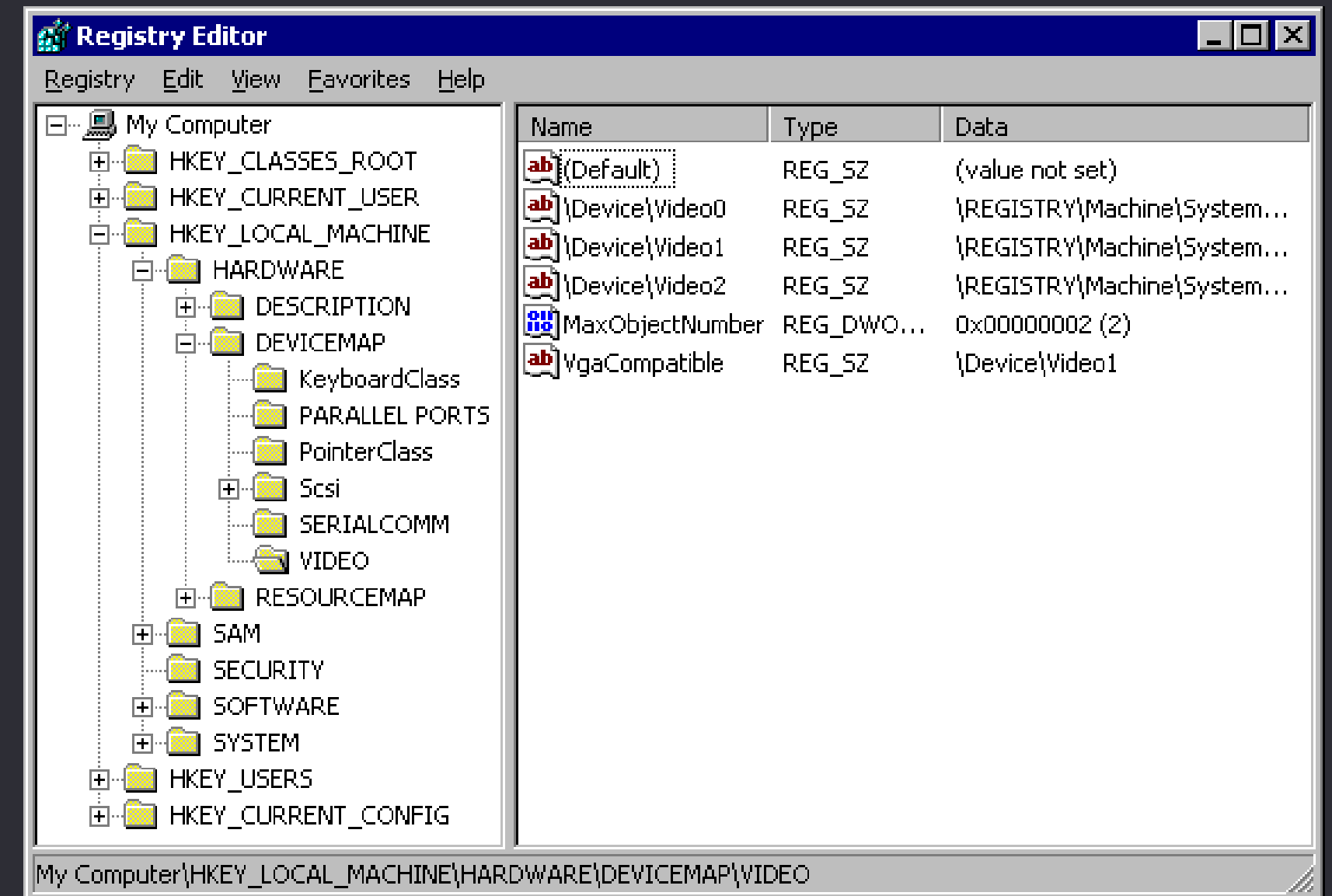


# Registro de windows (PEGRILOSO)

Dentro del OS windows tenemos una base de datos jerarquica donde se almacena la configuracion de programas y del sistema. Podemos alterar este registro para lograr que nuestro malware obtenga persitencia incluso si se reinicia la computadora.

La API nos deja crear y editar registros a voluntad.

<https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-functions>



}

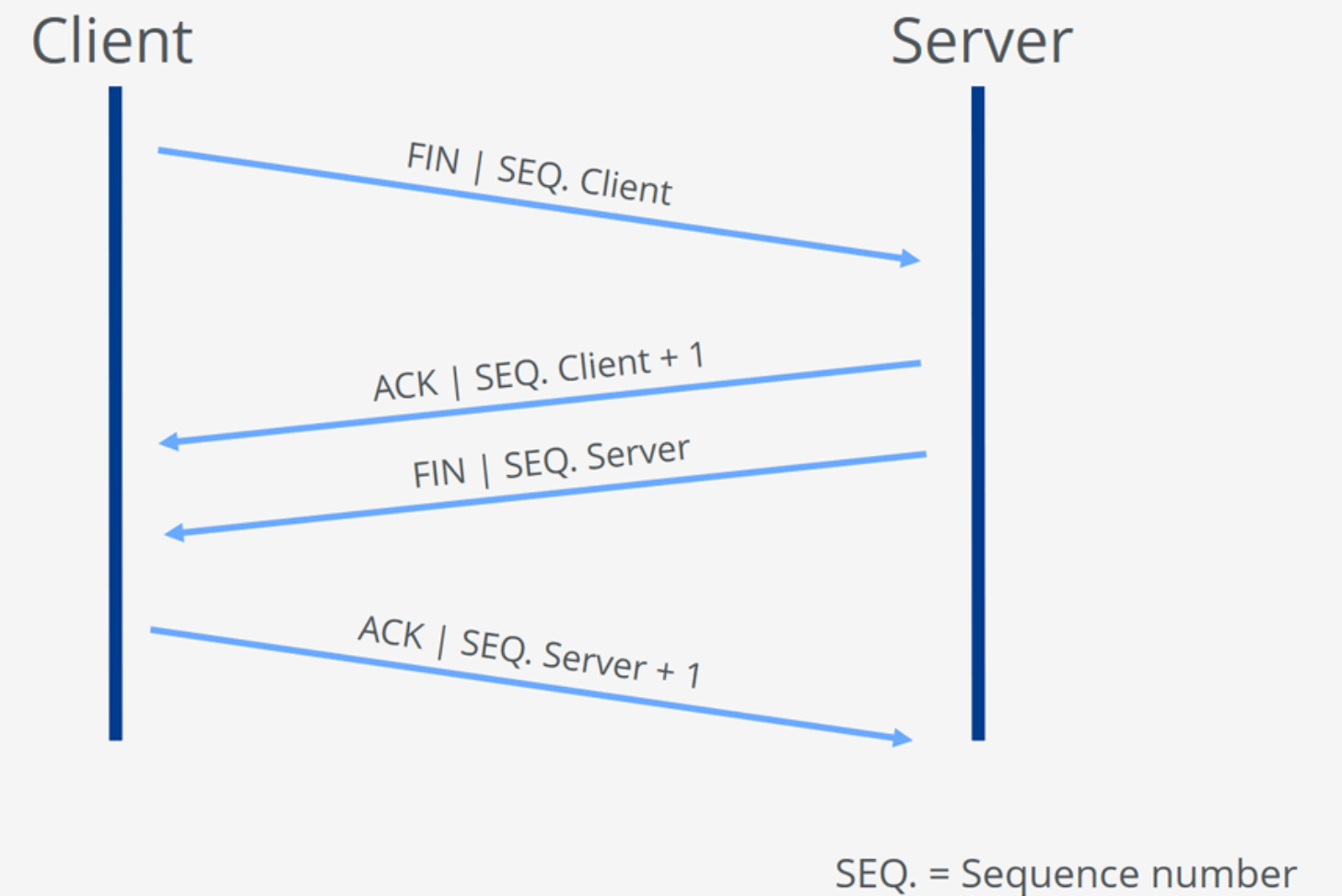
# Manipulacion de redes

La API de windows nos deja crear conexiones a otras redes de muchas maneras y protocolos.

Esto nos sirve para exfiltracion de datos y command and control de nuestro sistema.

<https://learn.microsoft.com/en-us/windows/win32/networking>

## TCP connection termination (TCP Teardown)

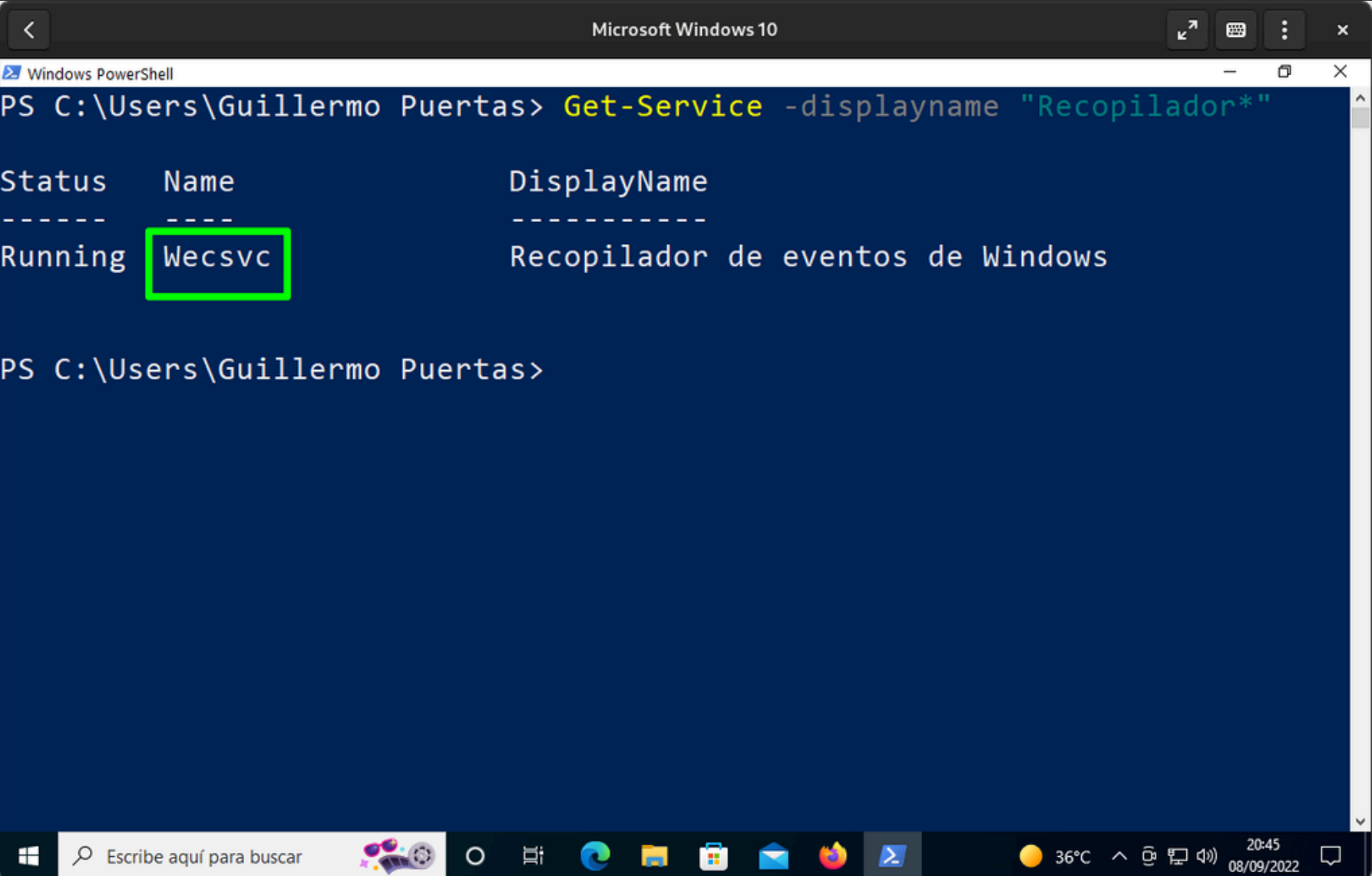


# Manipulacion de servicios

Un servicio es un procesos de windows que se ejecuta al inciar el sistema. Usualmente cargan con privilegios de ejecutivo y no de usuario. Modificar estos servicios es muy valioso para escalar privilegios y conseguir persistencia.

La API de windows nos deja editar estos servicios.

<https://learn.microsoft.com/en-us/windows/win32/services/service-functions>



```
Microsoft Windows 10
Windows PowerShell
PS C:\Users\Guillermo Puertas> Get-Service -displayname "Recopilador*"

Status      Name      DisplayName
-----
Running     Wecsvc    Recopilador de eventos de Windows

PS C:\Users\Guillermo Puertas>
```



# Hooks

Los hooks son una de las funciones mas utiles de la API de windows. Sirven como un filtro entre eventos del sistema.

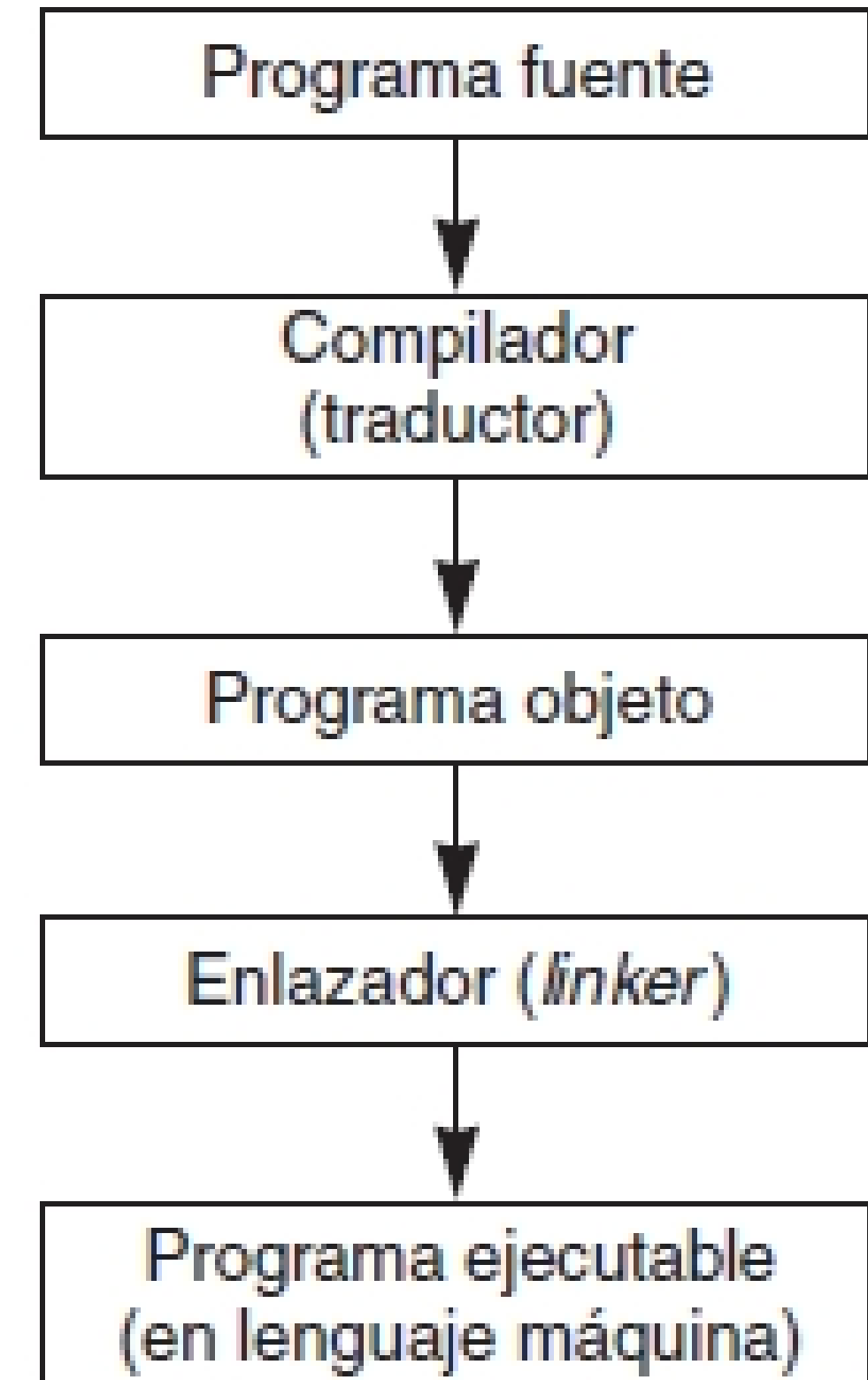
Podemos crearlos para monitorear ciertas acciones del usuario o sistema. Desde que teclas se precionan hasta inicio de procesos.

Para utilizar los hooks tenemos que instalarlos y luego dejarlos corriendo para que filtren todos los eventos que queramos alterar.

<https://learn.microsoft.com/en-us/windows/win32/services/service-functions>



# COMPILACION



# A PROGRAMAR TU PRIMER KEYLOGGER

