THALES

La fiabilité des logiciels anti-rookits Windows 32 bits

Thomas SABONO tsabono@lab.b-care.net

- Matériel
  - Pentium 4-M 2.20 Ghz
  - 1 Go Ram

- Systèmes d'exploitation
  - Windows XP professionnel Service Pack 2

- 3 hooks au niveau kernel

- Implémentation : Keylogger

1ére méthode : Hook IRP

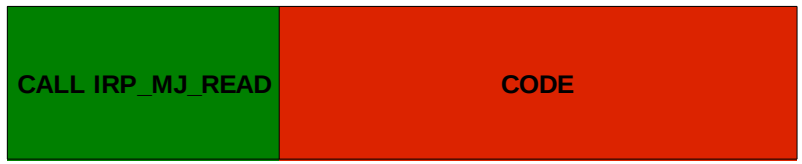
```
lkd> !drvobj kbdclass 2
Driver object (8423db20) is for:
 \Driver\Kbdclass
DriverEntry:   f7908610 kbdclass!GsDriverEntry
DriverStartIo: 00000000
DriverUnload:  00000000

Dispatch routines:
[00] IRP_MJ_CREATE                      f7904dd8    kbdclass!KeyboardClassCreate
[01] IRP_MJ_CREATE_NAMED_PIPE           804f4296    nt!IopInvalidDeviceRequest
[02] IRP_MJ_CLOSE                       f7904fe8    kbdclass!KeyboardClassClose
[03] IRP_MJ_READ                        f7905c82    kbdclass!KeyboardClassRead
[04] IRP_MJ_WRITE                       804f4296    nt!IopInvalidDeviceRequest
[05] IRP_MJ_QUERY_INFORMATION           804f4296    nt!IopInvalidDeviceRequest
[06] IRP_MJ_SET_INFORMATION             804f4296    nt!IopInvalidDeviceRequest
[07] IRP_MJ_QUERY_EA                    804f4296    nt!IopInvalidDeviceRequest
[08] IRP_MJ_SET_EA                      804f4296    nt!IopInvalidDeviceRequest
[09] IRP_MJ_FLUSH_BUFFERS               f7904d50    kbdclass!KeyboardClassFlush
[0a] IRP_MJ_QUERY_VOLUME_INFORMATION    804f4296    nt!IopInvalidDeviceRequest
[0b] IRP_MJ_SET_VOLUME_INFORMATION      804f4296    nt!IopInvalidDeviceRequest
[0c] IRP_MJ_DIRECTORY_CONTROL           804f4296    nt!IopInvalidDeviceRequest
[0d] IRP_MJ_FILE_SYSTEM_CONTROL         804f4296    nt!IopInvalidDeviceRequest
[0e] IRP_MJ_DEVICE_CONTROL              f7906a44    kbdclass!KeyboardClassDeviceControl
[0f] IRP_MJ_INTERNAL_DEVICE_CONTROL     f7906386    kbdclass!KeyboardClassPassThrough
[10] IRP_MJ_SHUTDOWN                    804f4296    nt!IopInvalidDeviceRequest
[11] IRP_MJ_LOCK_CONTROL                804f4296    nt!IopInvalidDeviceRequest
[12] IRP_MJ_CLEANUP                     f7904d0c    kbdclass!KeyboardClassCleanup
[13] IRP_MJ_CREATE_MAILSLOT             804f4296    nt!IopInvalidDeviceRequest
[14] IRP_MJ_QUERY_SECURITY              804f4296    nt!IopInvalidDeviceRequest
[15] IRP_MJ_SET_SECURITY                804f4296    nt!IopInvalidDeviceRequest
[16] IRP_MJ_POWER                       f7907196    kbdclass!KeyboardClassPower
[17] IRP_MJ_SYSTEM_CONTROL              f7906844    kbdclass!KeyboardClassSystemControl
[18] IRP_MJ_DEVICE_CHANGE               804f4296    nt!IopInvalidDeviceRequest
[19] IRP_MJ_QUERY_QUOTA                 804f4296    nt!IopInvalidDeviceRequest
[1a] IRP_MJ_SET_QUOTA                   804f4296    nt!IopInvalidDeviceRequest
[1b] IRP_MJ_PNP                         f7905798    kbdclass!KeyboardPnP
```

IRP : Paquet de requête d'entrée/sortie servant à la communication inter-drivers.

1ére méthode : Hook IRP

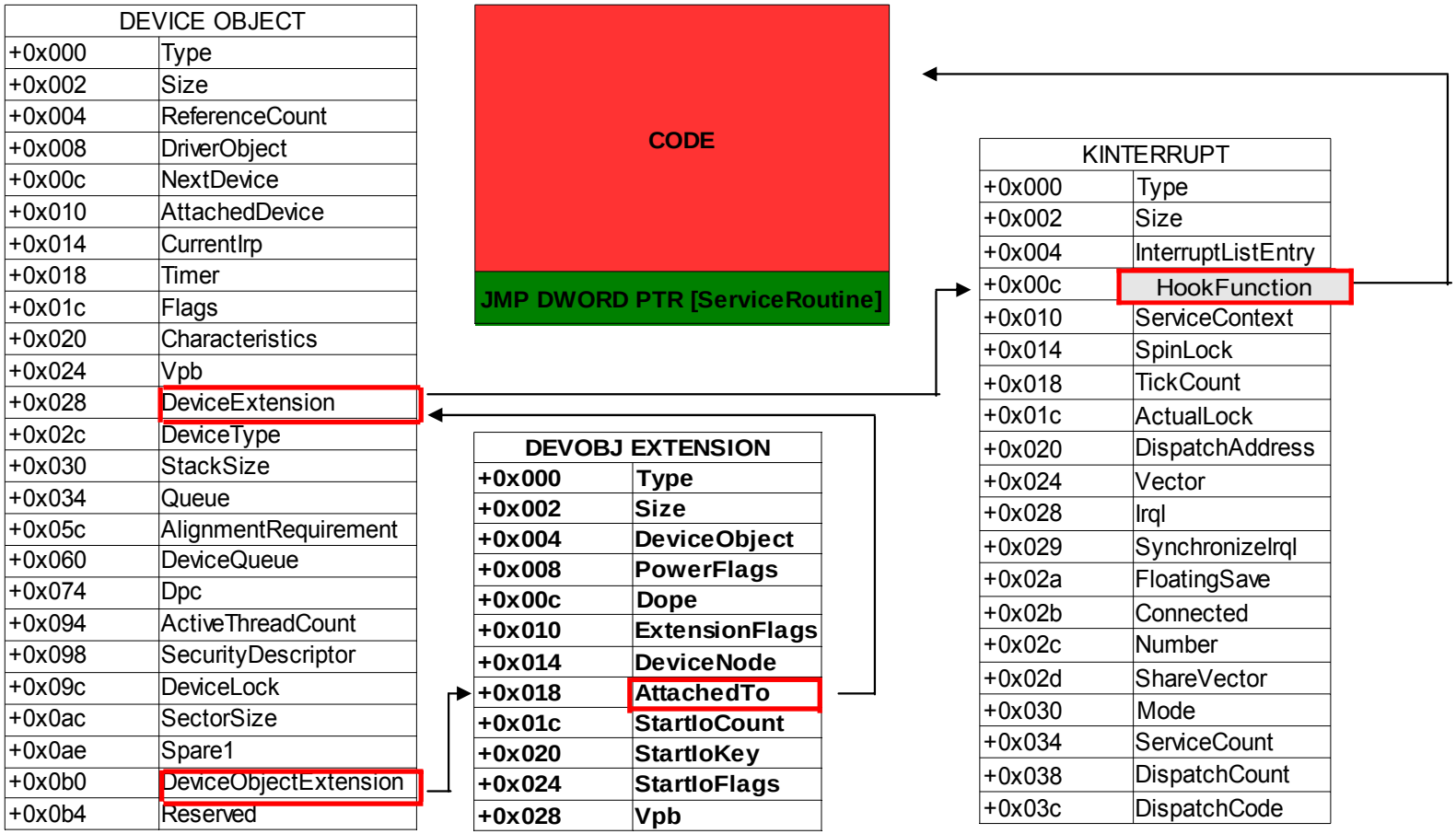
DEVICE OBJECT	
+0x000	Type
+0x002	Size
+0x004	ReferenceCount
+0x008	DriverObject
+0x00c	NextDevice
+0x010	AttachedDevice
+0x014	CurrentIrp
+0x018	Timer
+0x01c	Flags
+0x020	Characteristics
+0x024	Vpb
+0x028	DeviceExtension
+0x02c	DeviceType
+0x030	StackSize
+0x034	Queue
+0x05c	AlignmentRequirement
+0x060	DeviceQueue
+0x074	Dpc
+0x094	ActiveThreadCount
+0x098	SecurityDescriptor
+0x09c	DeviceLock
+0x0ac	SectorSize
+0x0ae	Spare1
+0x0b0	DeviceObjectExtension
+0x0b4	Reserved

DRIVER OBJECT	
+0x000	Type
+0x002	Size
+0x004	DeviceObject
+0x008	Flags
+0x00c	DriverStart
+0x010	DriverSize
+0x014	DriverSection
+0x018	DriverExtension
+0x01c	DriverName
+0x024	HardwareDatabase
+0x028	FastIoDispatch
+0x02c	DriverInit
+0x030	DriverStartIo
+0x034	DriverUnload
+0x038	MajorFunction



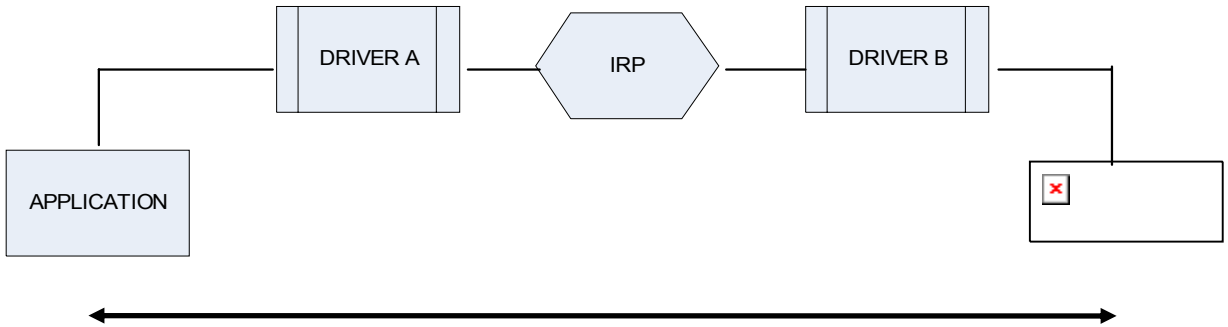
IRP : Paquet de requête d'entrée/sortie servant à la communication inter-drivers.

2éme méthode : Hook ISR

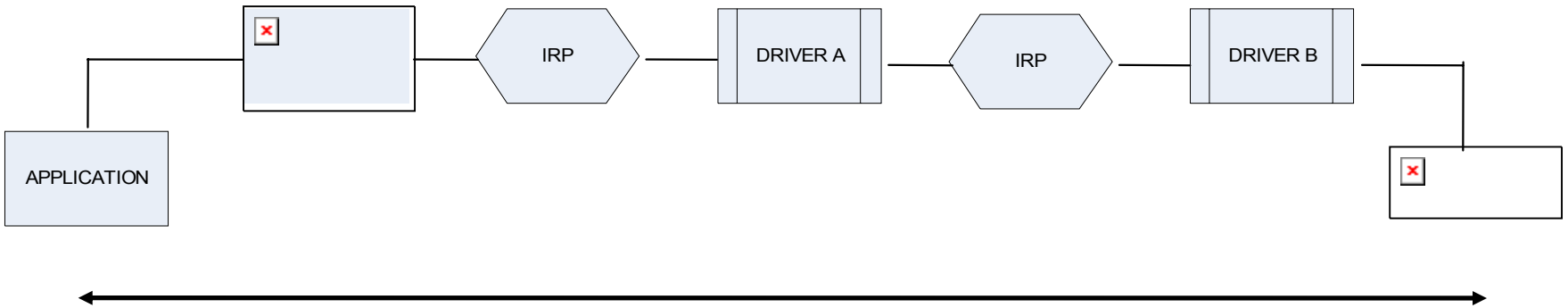


ISR : Routine exécuté au déclenchement d'une interruption.

3éme méthode : Chaînage drivers



3éme méthode : Chaînage drivers



Résultats des tests

	Hook ISR	Hook IRP	Chaînage drivers
Darkspy			
Rootkit Revealer			
RAIDE			
F-Secure Blacklight			
GMER		×	
Sophos Anti-Rootkit			
AVG Anti-Rootkit			
Bit defender Uncover			
Rootkit hook analyzer			
Panda Anti-rootkit			
McAfee rootkit Detective			

Furtivité :

- Méthode dynamique > méthode statique
- Mode kernel

Détection/Protection :

- Drivers signés
- Adresse appartenant à des modules légitimes

THANKS !