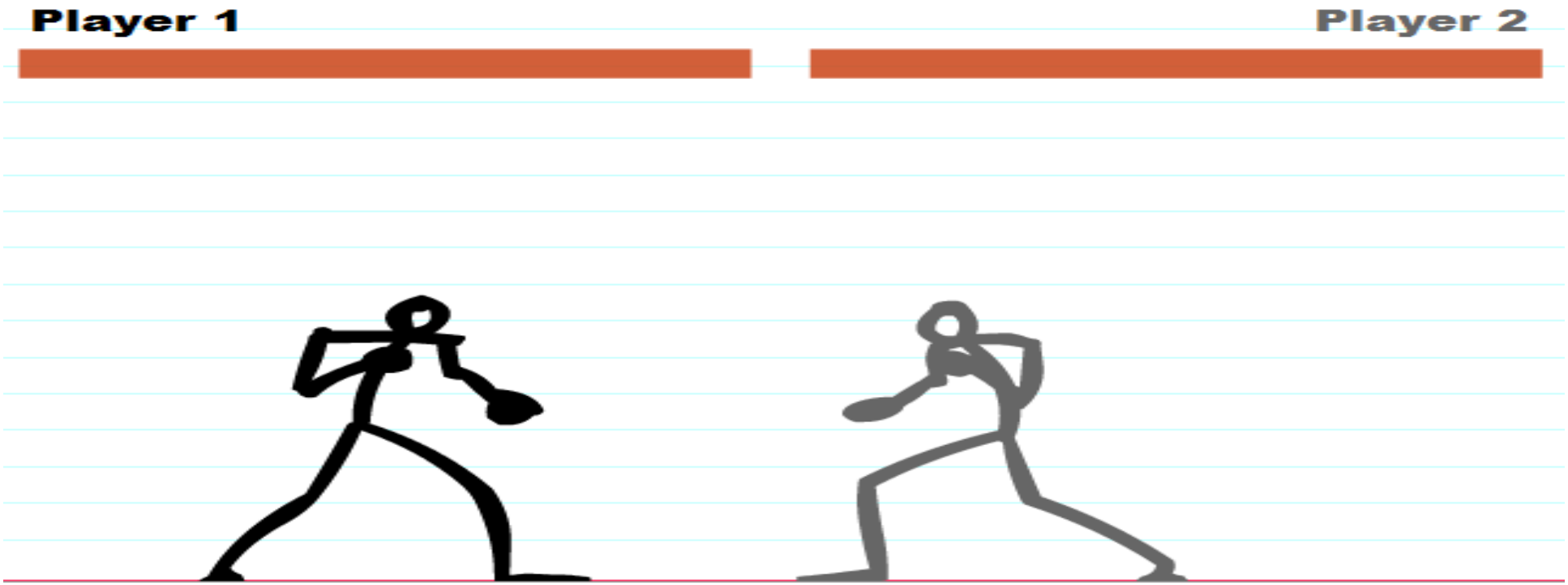
兵家必爭之地

Nanika

- 在防毒與惡意軟體間的一往一來就是一場激烈的戰爭
- 在一黑一白對抗之中各有輸贏



- 安全需要對於任何風險都略懂
- 知彼知己，百戰不殆；不知彼而知己，一勝一負；不知彼，不知己，每戰必殆
- 知識就是力量

守方優劣勢

- 先常駐在系統,掌握各個關鍵關口,並且對於任何變動都可以瞭若指掌,擁有龐大的資源,發現新攻擊方式會使用各種技巧封阻

- 以穩定度為核心並且不能作太細膩的檢查影響效能,不能使用不穩定的先進技術,守勢地圖直接攤在外面讓人研究

掌握關鍵關口

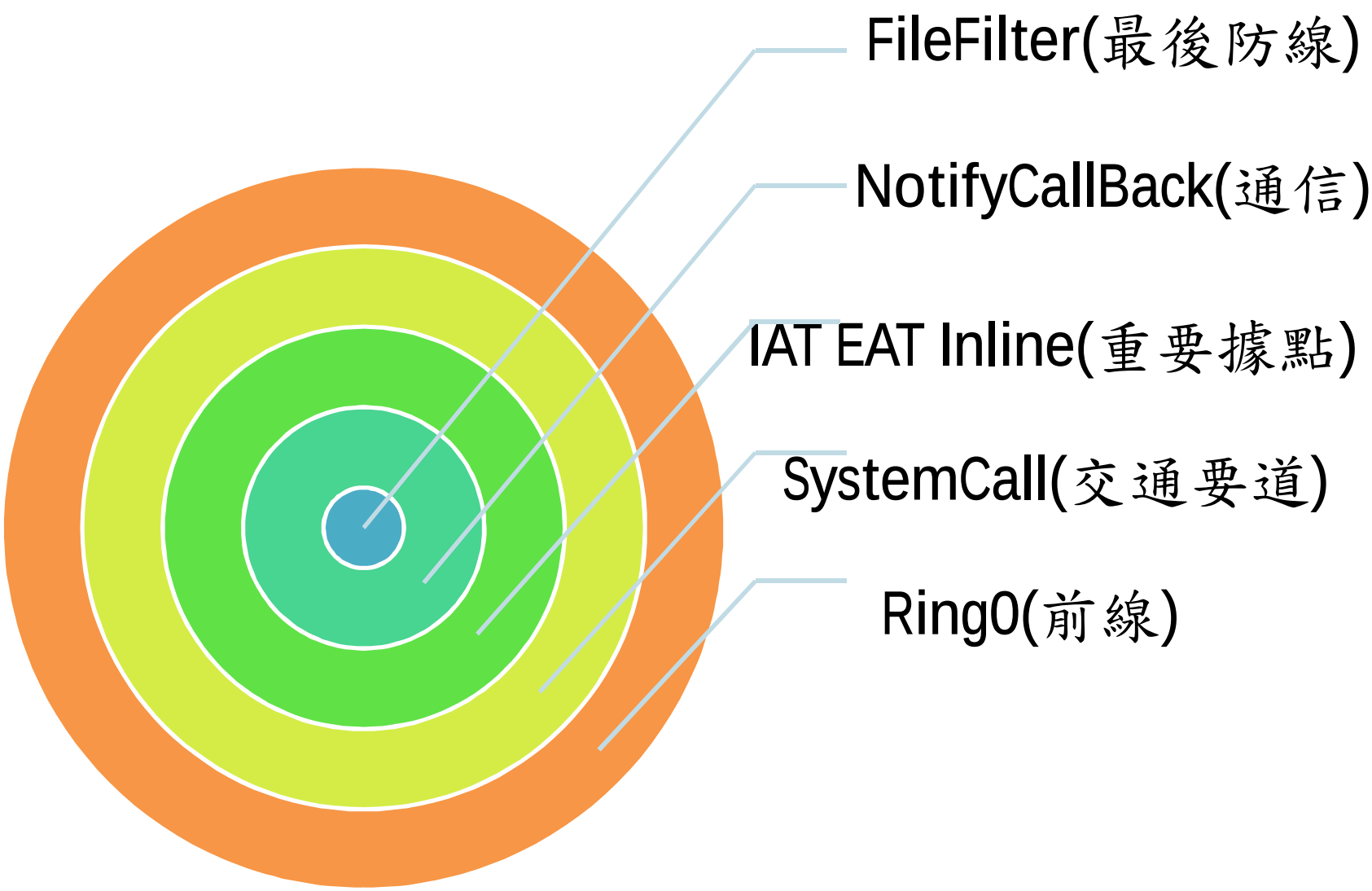
守勢地圖公開

攻方優劣勢

- 各種技巧不需要以穩定為核心，需依照守勢地圖找新計謀突破，當守勢很完備的時候則需要使用些奇淫技巧

- 沒辦法準確的瞭解攻擊目標的環境，常常一公開新技巧馬上會被封阻，沒辦法一勞永逸

必爭之地



Ring0(突破前線)

- 替換REG
- 替換檔案
- \Device\PhysicalMemory
- ZwLoadDriver
- ZwSystemDebugControl
- ZwSetSystemInformation
- Kernel Bug
- .....

嘿嘿 走後門
我最在行

惡意表情

兵不厭詐
這是戰爭

突破前線後要怎樣進攻

- 正面突破
- 各個擊破

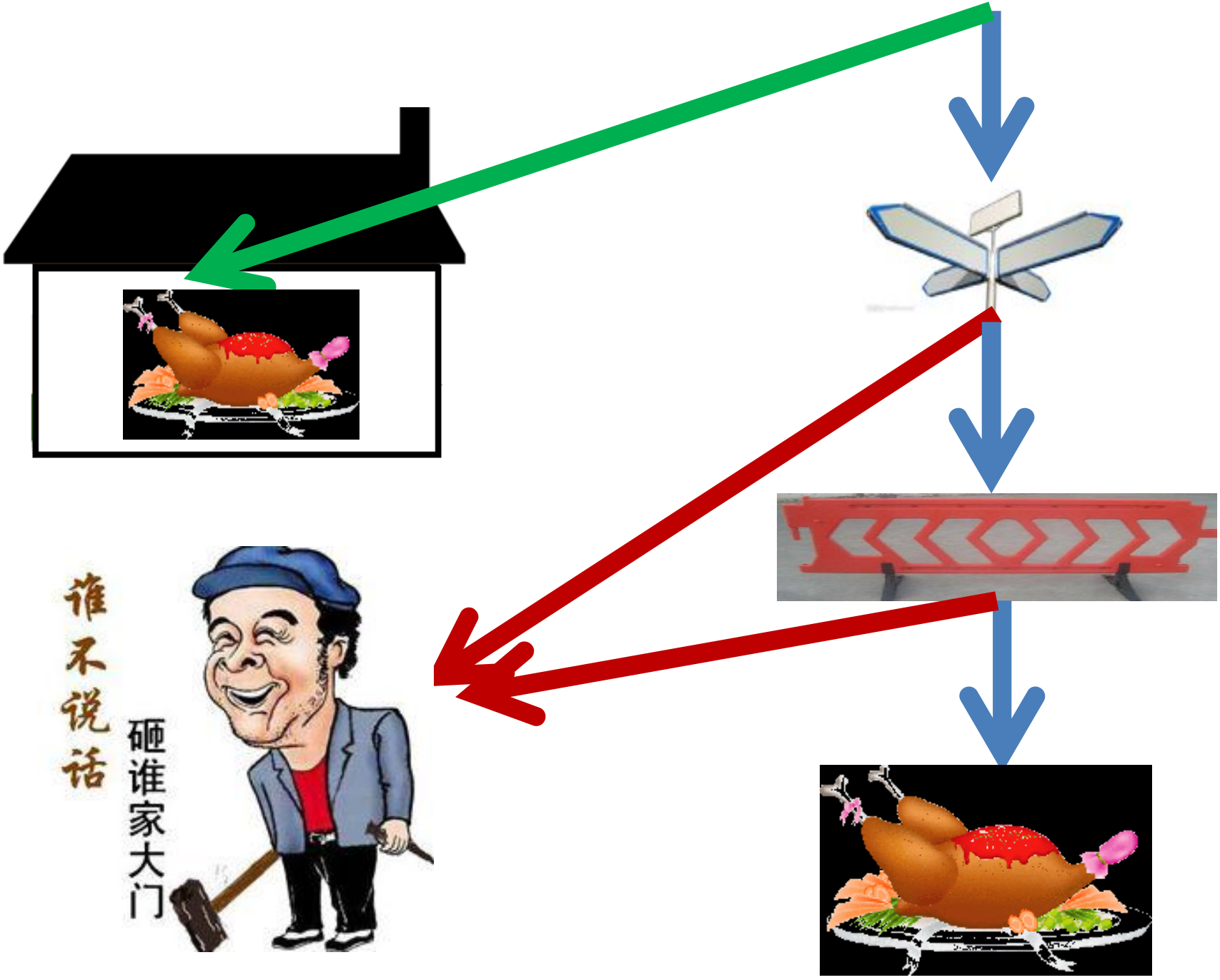
正面突破(MmUnloadSystemImage)

各個擊破

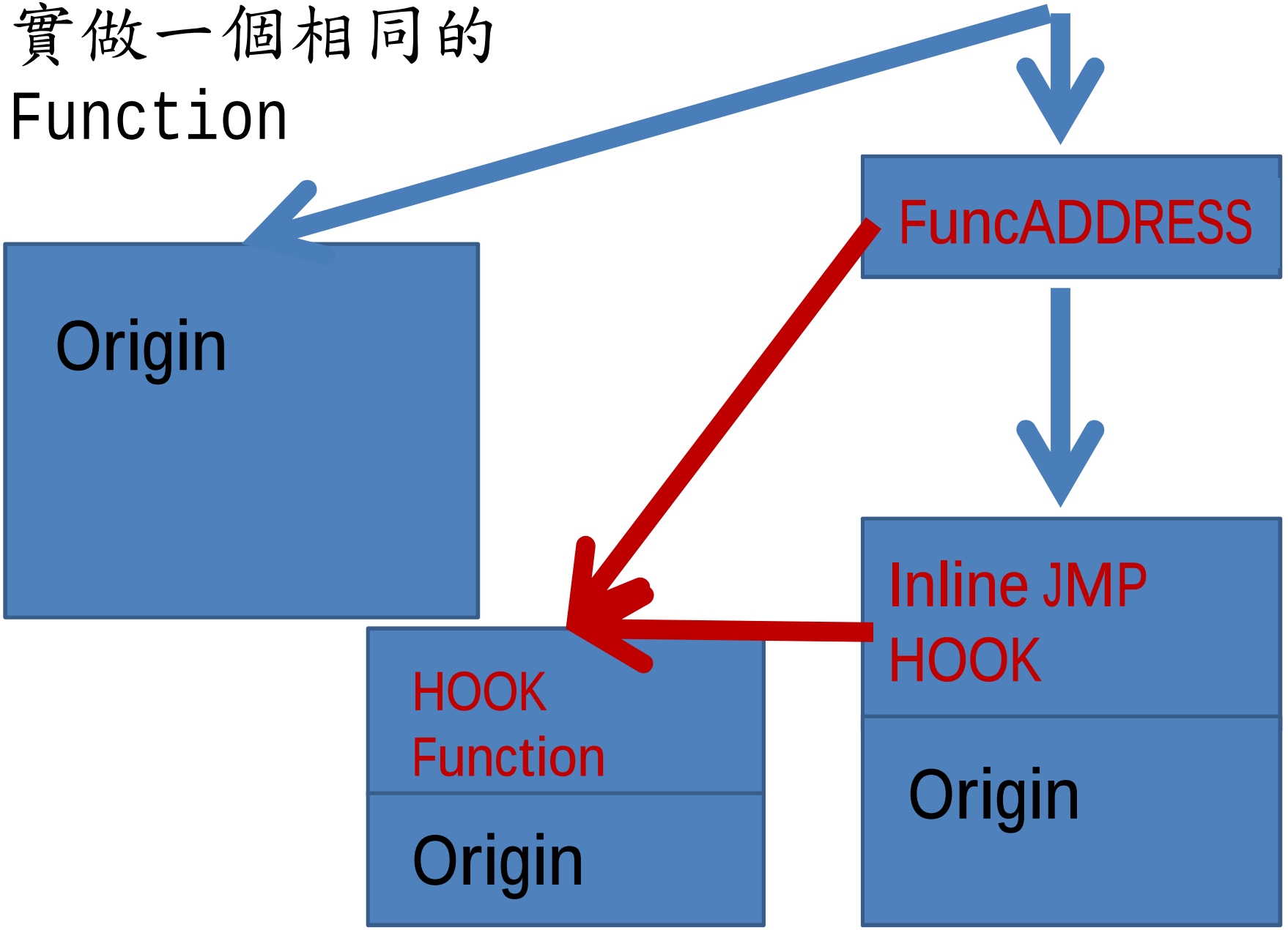
- 分析守勢地圖後精準突破

SystemCall(交通要道)

- SSDT (實做一整個Function)(還原)
- Inline Hook(實做一整個Function)(還原)
- 攔截與還原的無窮迴圈



實做一個相同的Function



IAT EAT Inline(重要據點)

- MmGetSystemRoutineAddress
- IofCallDriver
- ObReferenceObjectbyName
- KeUserModeCallBack
- ……
- 實做一整個Function or 還原
- 各家有各家的喜好又是攔截與還原的無窮迴圈

NotifyCallBack(通信)

- PsSetCreateProcessNotifyRoutine
- PsSetCreateThreadNotifyRoutine
- PsSetLoadImageNotifyRoutine
- CmRegisterCallback
- 中斷通訊爲戰爭必備攻勢

報告長官,偵測到新的Process,快進行掃描

截斷通信

- PsSetCreateProcessNotifyRoutine(PCREATE_PROCESS_NOTIFY_ROUTINE NotifyRoutine, BOOLEAN Remove)
- PAGE:004EEE96 mov edi, edi
- PAGE:004EEE98 push ebp
- PAGE:004EEE99 mov ebp, esp
- PAGE:004EEE9B push ebx
- PAGE:004EEE9C xor ebx, ebx
- PAGE:004EEE9E cmp [ebp+Remove], bl
- PAGE:004EEEA1 push esi
- PAGE:004EEEA2 push edi
- PAGE:004EEEA3 jz short loc_4EEF0A
- PAGE:004EEEA5 mov edi, offset byte_483360
- 找出所有Routine 之後移除列表

FileFilter(最後防線)

- FltRegisterFilter
- FSD Routine
- IoAttachDevice
- 最後防線突破等於攻下城池

- dt nt!_driver_object 816565e0
- +0x000 Type : 4
- +0x002 Size : 168
- +0x004 DeviceObject : 0x8147b030 _DEVICE_OBJECT
- +0x008 Flags : 0x12
- +0x00c DriverStart : 0xf8262000
- +0x010 DriverSize : 0x58480
- +0x014 DriverSection : 0x816cc230
- +0x018 DriverExtension : 0x81656688 _DRIVER_EXTENSION
- +0x01c DriverName : _UNICODE_STRING "\Driver\Tcpip"
- +0x024 HardwareDatabase : 0x80671b60 _UNICODE_STRING "\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\SYSTEM"
- +0x028 FastIoDispatch : (null)
- +0x02c DriverInit : 0xf82b2d23 long tcpip!GsDriverEntry+0
- +0x030 DriverStartIo : (null)
- +0x034 DriverUnload : 0xf8290a58 void tcpip!ArpUnload+0
- +0x038 MajorFunction : [28] 0xf82684f9 long tcpip!TCPDispatch+0

透過檔案比對恢復FSD MajorFunction

- +0x038 MajorFunction : [0] 0xf82684f9 long tcpip!TCPDispatch+0

```
INIT:00095470                call    ds:IoCreateDevice
INIT:00095476                cmp     eax, ebx
INIT:00095478                jl      loc_95A79
INIT:0009547E                mov     dword ptr [esi+7Ch], offset loc_89CE9
INIT:00095485                mov     dword ptr [esi+68h], offset loc_381BD
INIT:0009548C                mov     dword ptr [esi+50h], offset loc_13ABB
INIT:00095493                mov     dword ptr [esi+38h], offset loc_35E01
INIT:0009549A                mov     dword ptr [esi+40h], offset loc_352EA
INIT:000954A1                mov     dword ptr [esi+44h], offset loc_12F2F
INIT:000954A8                mov     dword ptr [esi+48h], offset loc_11B4B
INIT:000954AF                mov     dword ptr [esi+5Ch], offset loc_500E5
INIT:000954B6                mov     dword ptr [esi+6Ch], offset loc_3A958
INIT:000954BD                mov     dword ptr [esi+80h], offset loc_35CB8
INIT:000954C7                mov     dword ptr [esi+78h], offset off_247F2
INIT:000954CE                mov     dword ptr [esi+0A4h], offset loc_52A0E
```

DriverObject->MajorFunction[IRP_MJ_CREATE] = KDispatchCreateClose;
DriverObject->MajorFunction[IRP_MJ_CLOSE] = KDispatchCreateClose;
DriverObject->MajorFunction[IRP_MJ_DEVICE_CONTROL] = KDispatchIoctl;

- dt nt!_driver_object 816565e0
- +0x000 Type : 4
- +0x002 Size : 168
- +0x004 DeviceObject : 0x8147b030 _DEVICE_OBJECT
- +0x008 Flags : 0x12
- +0x00c DriverStart : 0xf8262000
- +0x010 DriverSize : 0x58480
- +0x014 DriverSection : 0x816cc230
- +0x018 DriverExtension : 0x81656688 _DRIVER_EXTENSION
- +0x01c DriverName : _UNICODE_STRING "\Driver\Tcpip"
- +0x024 HardwareDatabase : 0x80671b60 _UNICODE_STRING "\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\SYSTEM"
- +0x028 FastIoDispatch : (null)
- +0x02c DriverInit : 0xf82b2d23 long tcpip!GsDriverEntry+0
- +0x030 DriverStartIo : (null)
- +0x034 DriverUnload : 0xf8290a58 void tcpip!ArpUnload+0
- +0x038 MajorFunction : [28] 0xf82684f9 long tcpip!TCPDispatch+0

- kd> dt nt!_device_object 0x8147b030
- +0x000 Type : 3
- +0x002 Size : 0xb8
- +0x004 ReferenceCount : 2
- +0x008 DriverObject : 0x816565e0 _DRIVER_OBJECT
- +0x00c NextDevice : 0x81477030 _DEVICE_OBJECT
- +0x010 AttachedDevice : Null

- kd> dt nt!_device_object 0x 81477030
- +0x000 Type : 3
- +0x002 Size : 0xb8
- +0x004 ReferenceCount : 2
- +0x008 DriverObject : 0x816565e0 _DRIVER_OBJECT
- +0x00c NextDevice : 0x814e4030 _DEVICE_OBJECT
- +0x010 AttachedDevice : Null

眼花撩亂

真真假假假假真真

- 守方若需要守的完備需要花費大量的資源投入在相關的路線規劃上
- 攻方則需要更大量測試任何天馬行空的幻想
- 技術是一體兩面的,可以拿來防護,當然也可以知道怎樣攻擊

naninb@gmail.com

NET HACK

謝謝

Reference

- http://hi.baidu.com/sudami
- http://hi.baidu.com/mj0011
- http://www.debugman.com/
- http://forum.eviloctal.com/archiver/tid-33451.html
- 特別感謝我引用圖片的作者