EDR 致盲大作戰：解密 APT 攻擊中的 Evasion 藝術

CYCRAFT
奧 義 智 慧 科 技

趙偉捷 / oalieno

- 現為**奧義智慧**資安研究員
- 專注於**惡意程式分析**以及**沙盒系統開發**
- 畢業於**台灣大學**電機所資安碩士班
- 於 HITCON、CODEBLUE、IEEE DSC、SECCON 等研討會發表研究
- 於第二十六、二十七屆 **DEFCON CTF** 與 BFS 戰隊、BFKinesiS 聯隊獲得第十二名與第二名的成績
- 於 **Flareon9** 逆向工程挑戰中獲得獎章

APT (Advanced Persistent Threat)

新聞

您現在位置：首頁 > 新聞

超強後門！中國APT攻擊者「黑木」已潛伏5年以上

2024 / 01 / 29 - 編輯部

https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10923

< APT 攻擊 > " 有本事就來抓我啊~" 駭客平均躲藏天數 205 天

2015 年 08 月 07 日 趨勢科技 TrendMicro APT / APT攻擊 / APT 進階持續性威脅/ Advanced Persistent Threat

APT 駭客如何在你周圍四處遊走而不被發現

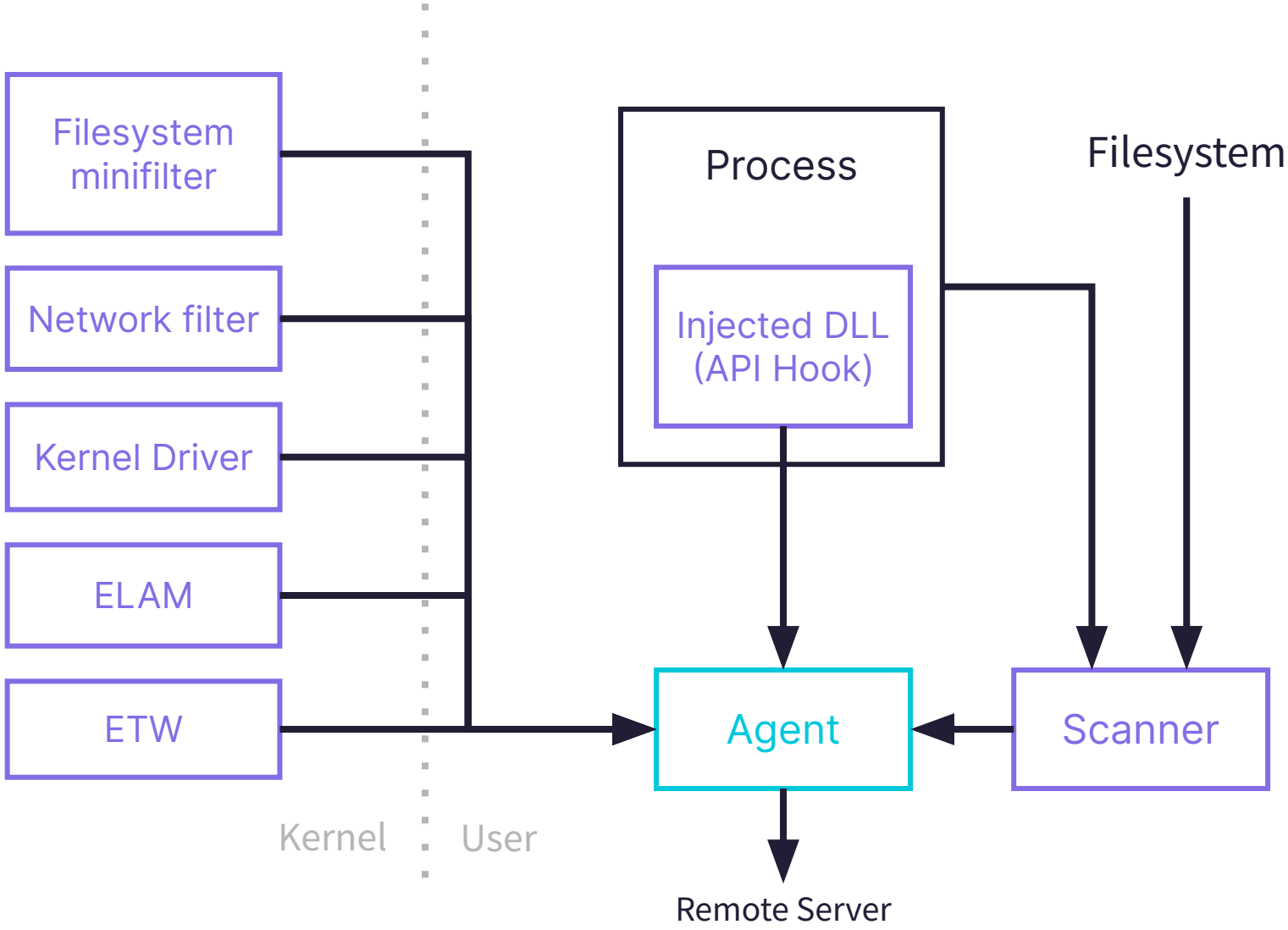
https://blog.trendmicro.com.tw/?p=13483

大綱

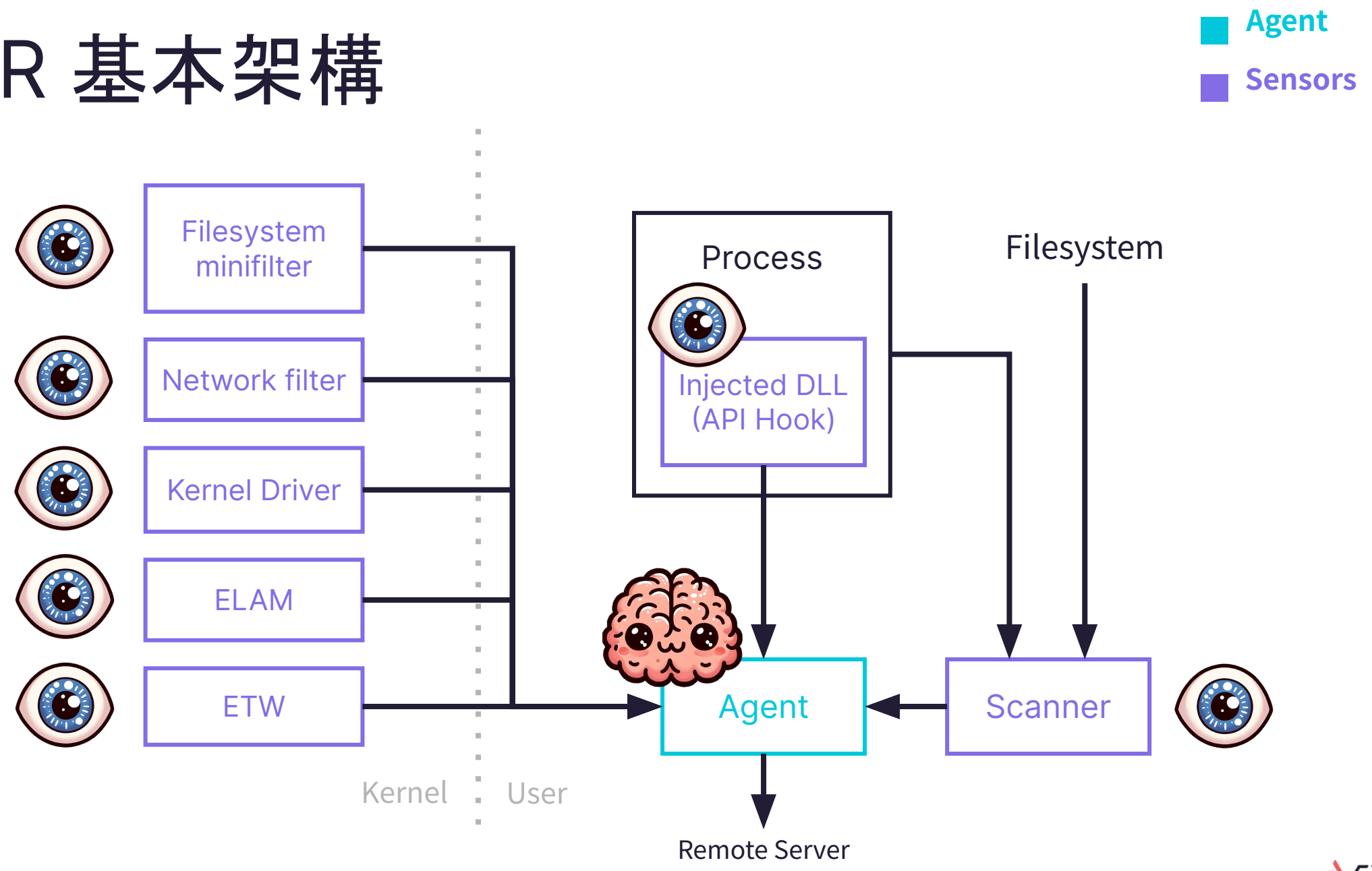
- EDR 怎麼運作
  - EDR 基本架構
  - 被動躲避和主動繞過的優缺點
- 實際 APT 案例剖析
  - 高科技產業 APT 案例
- Evasion 技術深入解析
  - API Hooking 的攻防戰
  - PPID Spoofing 只是 feature?

EDR 怎麼運作

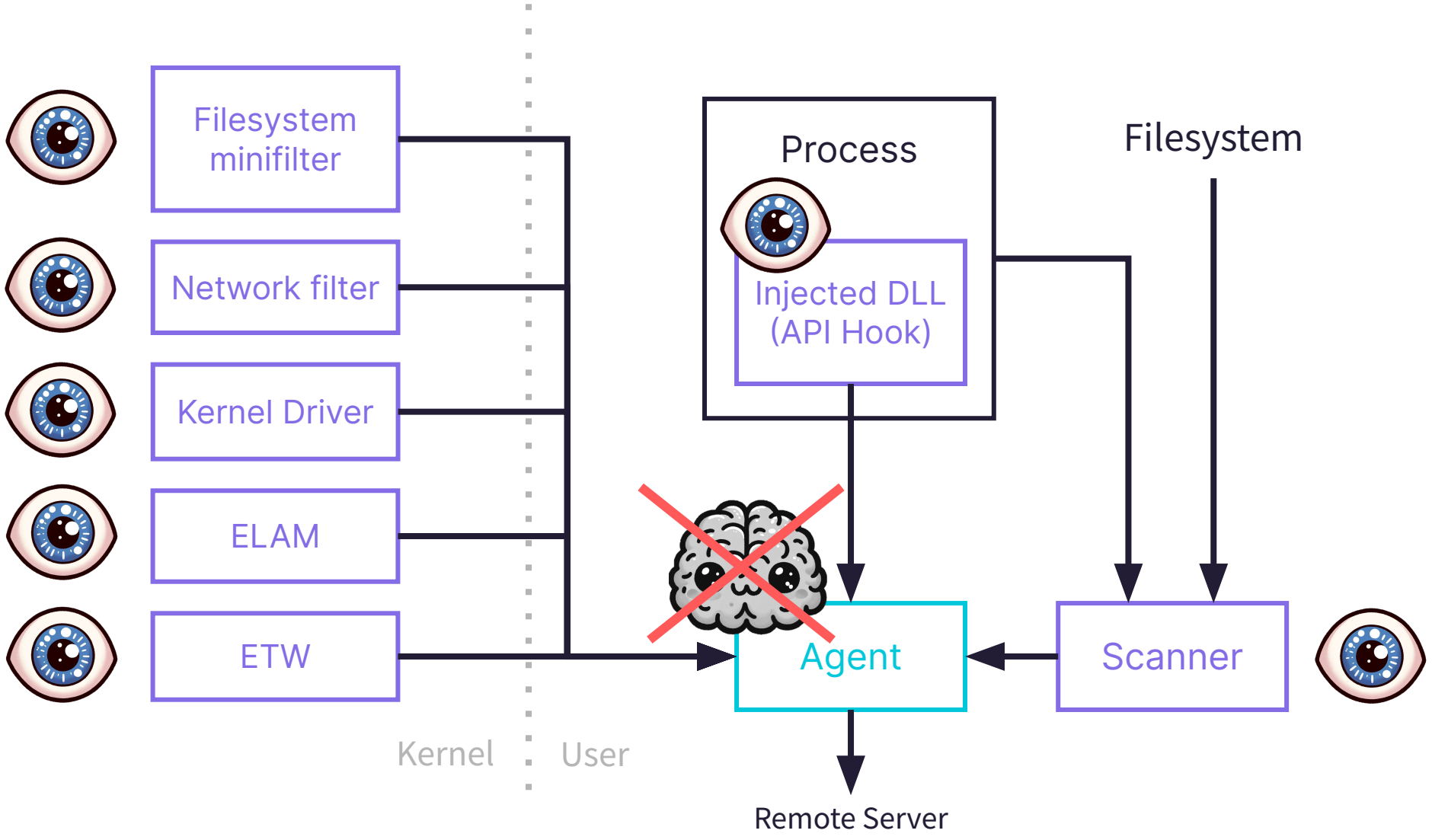
EDR 基本架構



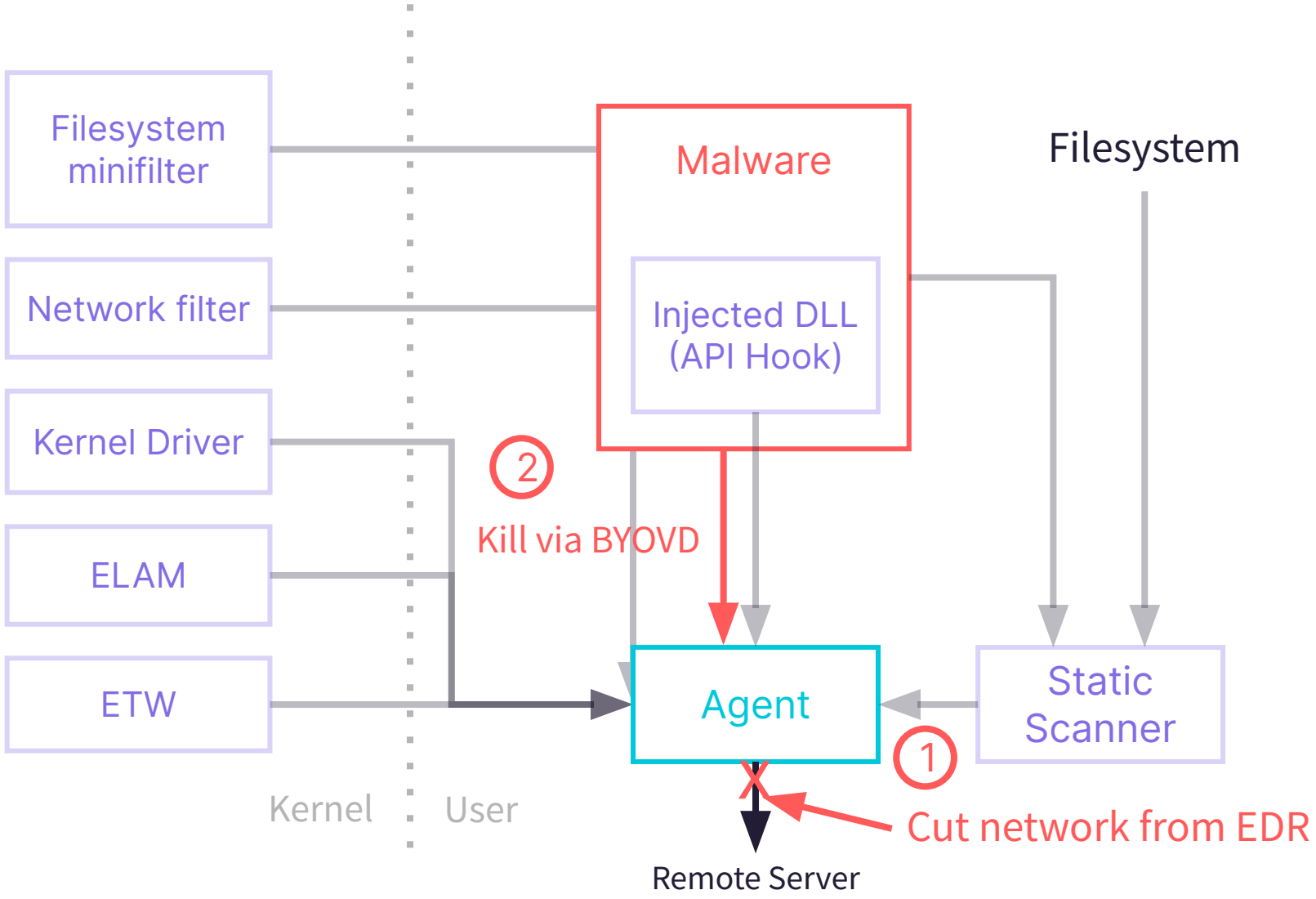
EDR 基本架構



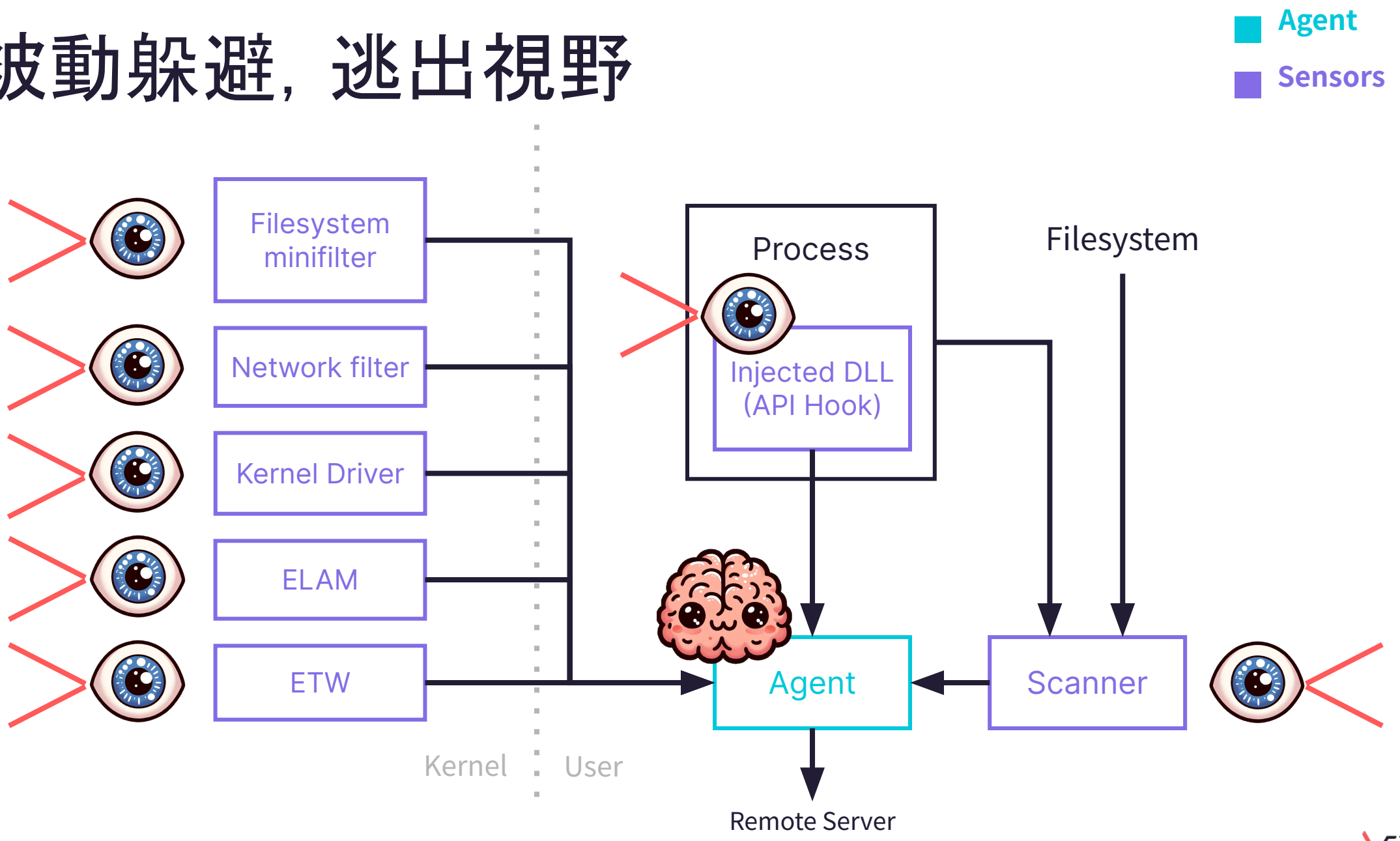
主動出擊，廢掉大腦



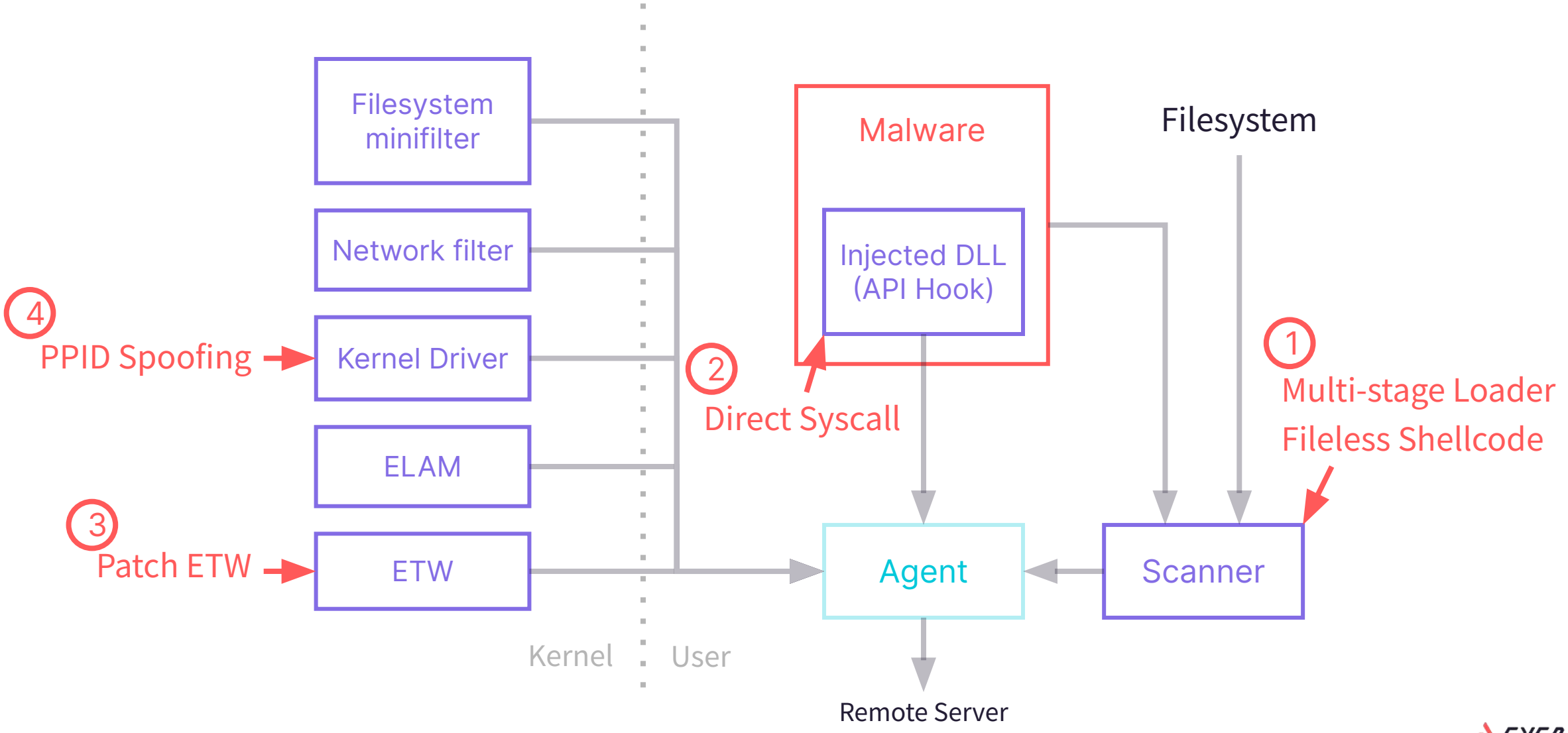
主動出擊



被動躲避，逃出視野



被動躲避

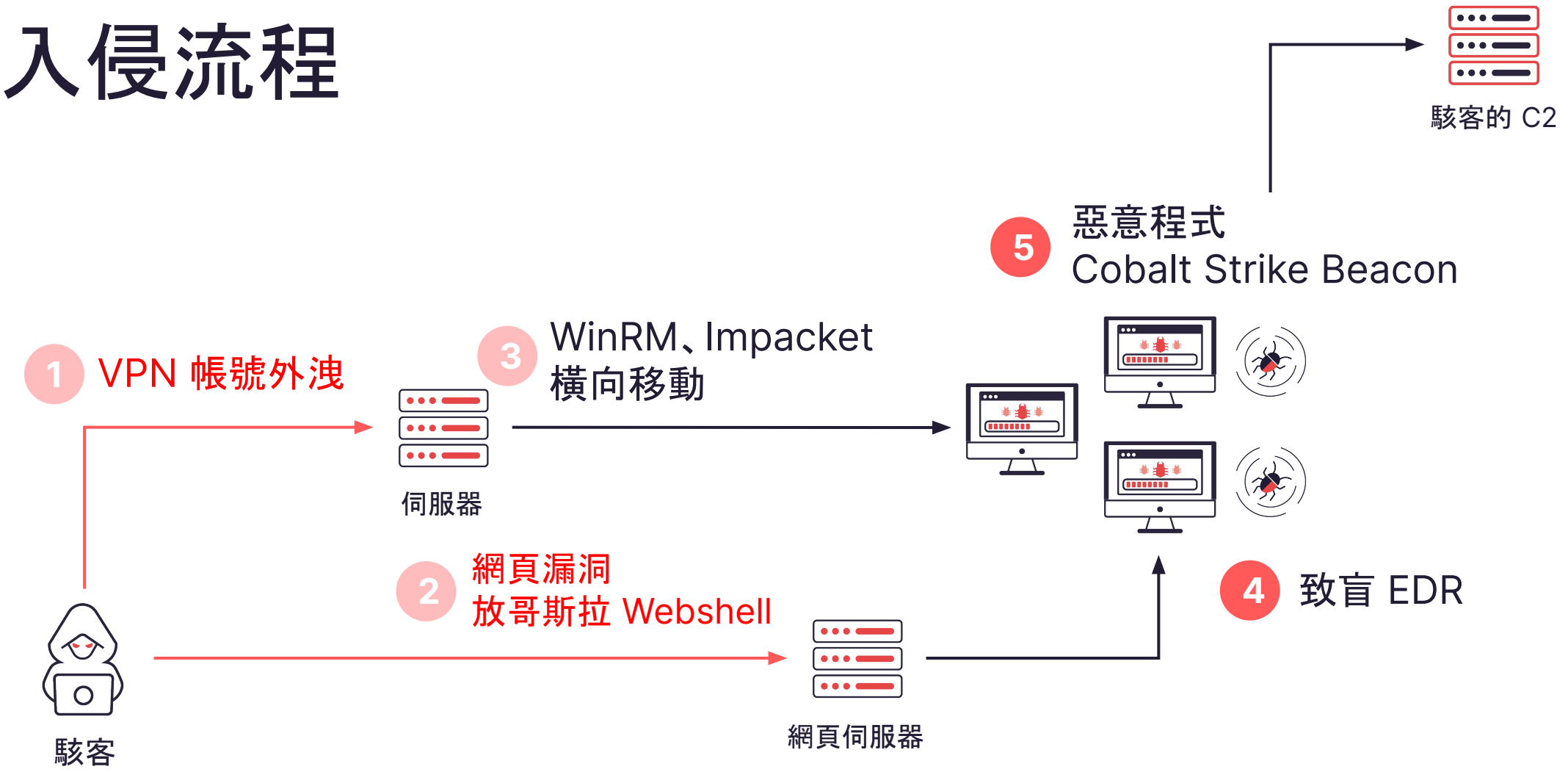


實際 APT 案例剖析

前情提要

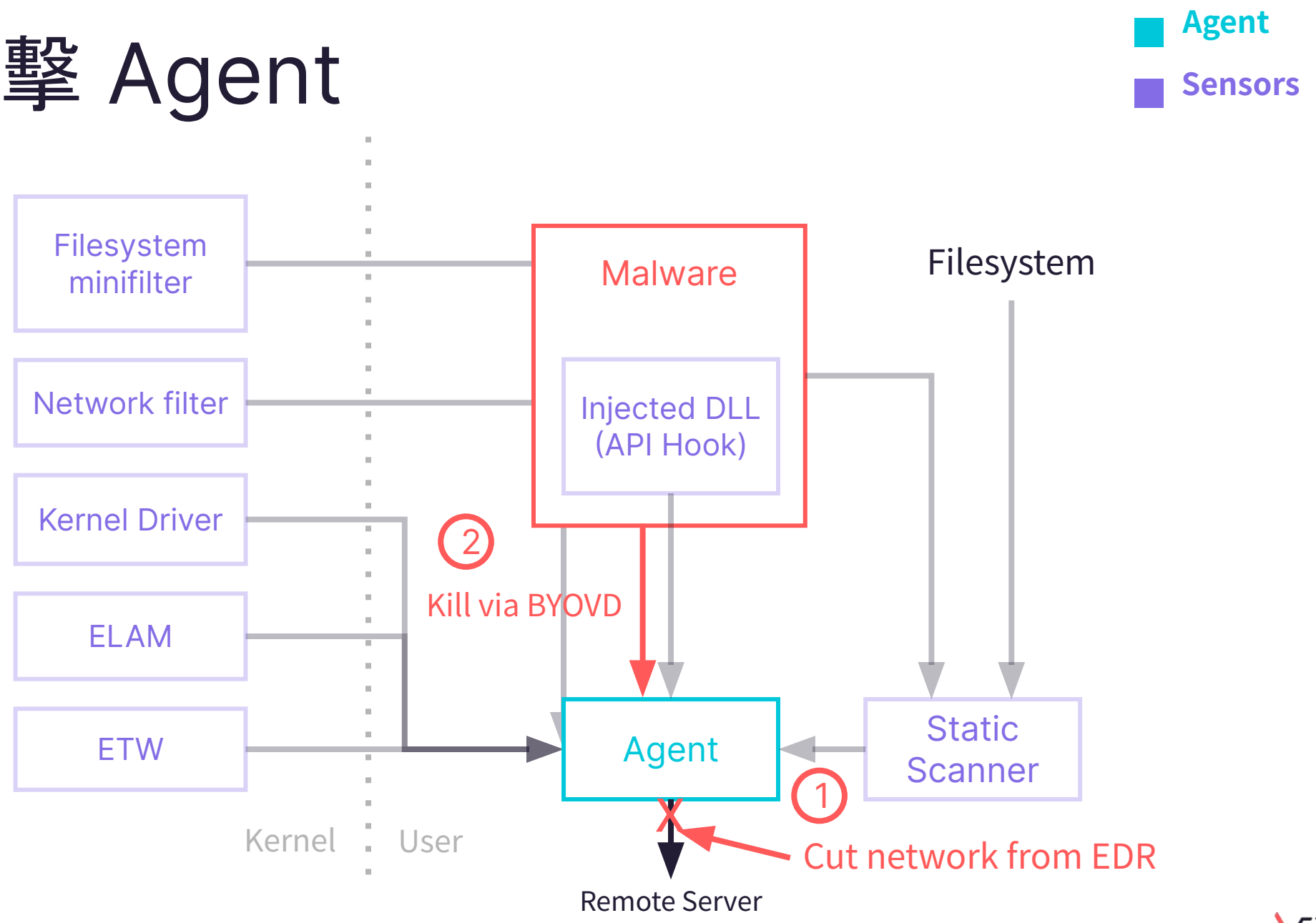
- 高科技產業
- 發現網路怪怪的，懷疑有駭客入侵
- 請求我們協助做鑑識調查，發現有被埋 webshell
- 我們檢查了整個系統，追查出惡意程式和 Cobalt Strike 後門

入侵流程



致盲 EDR

主動出擊 Agent



竄改 /etc/hosts

```
echo 1.5.3.4 securedr.com >> C:\Windows\System32\drivers\etc\hosts
netsh  advfirewall firewall add rule name=BlockIP dir=out action=block remoteip=1.2.3.4
```

Kill EDR (using BYOVD)

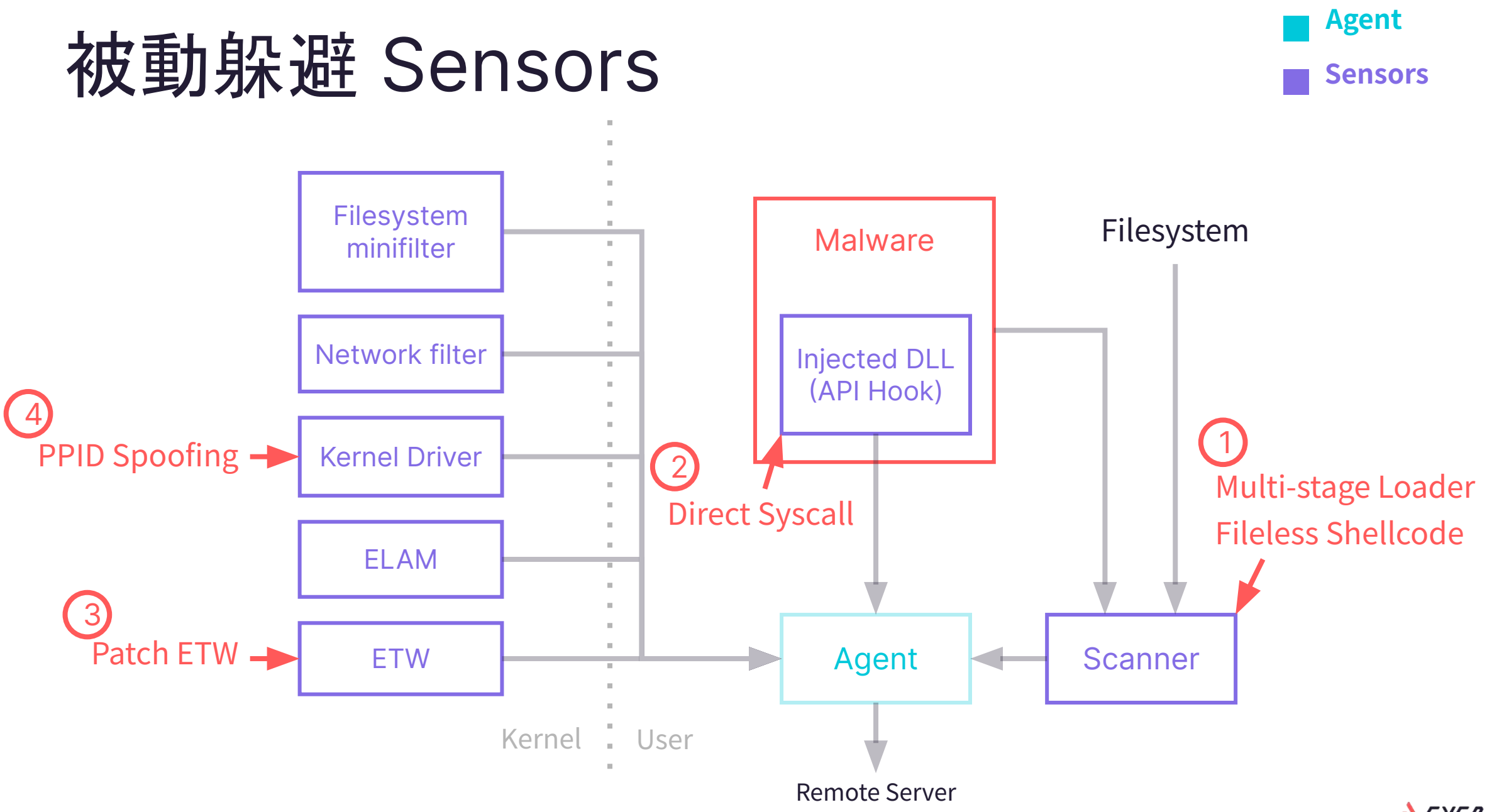
ReCryptLLC/CVE-2022-42045 (github.com)

BYOVD

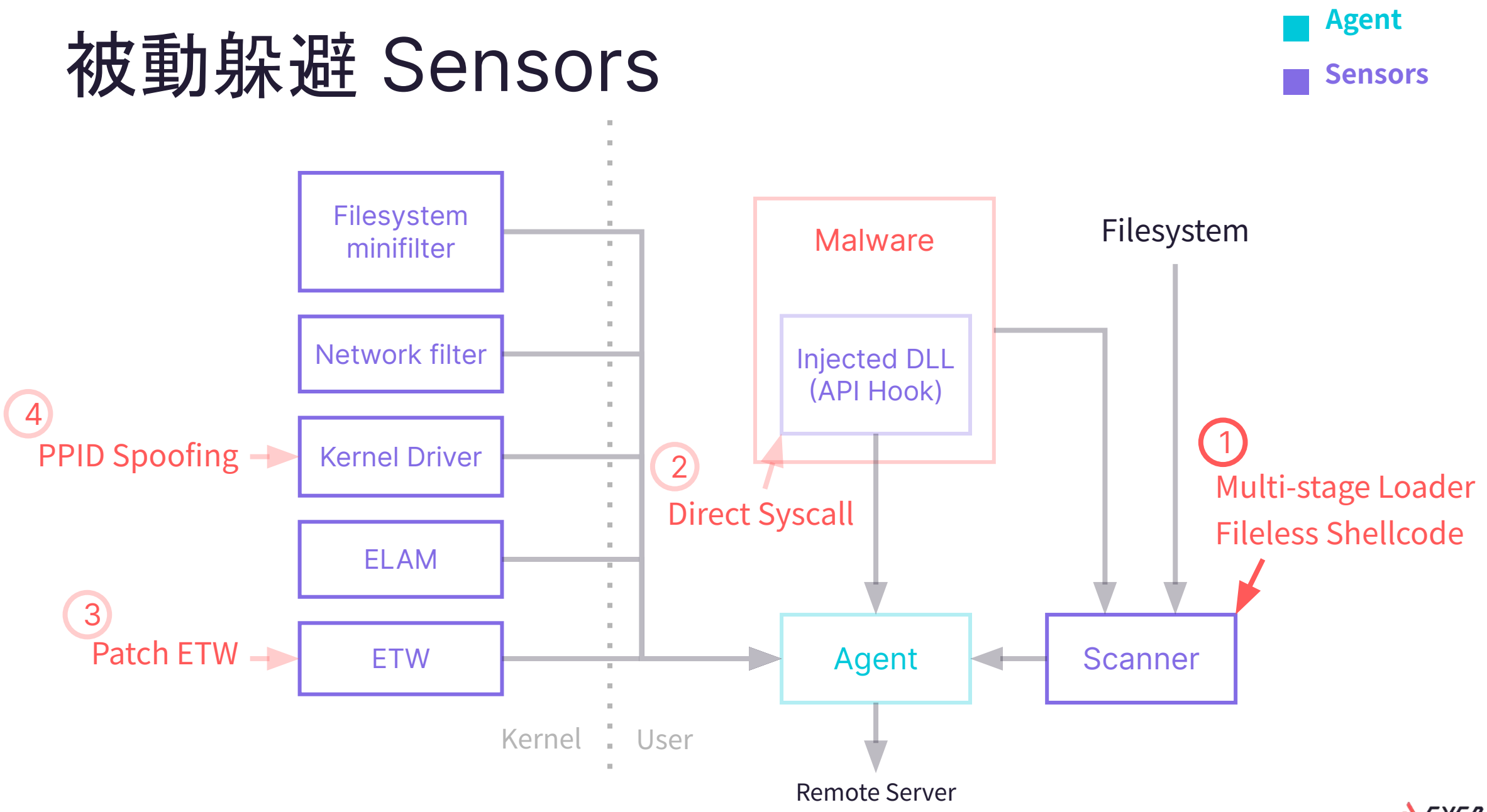
https://ithelp.ithome.com.tw/articles/10333769

惡意程式分析

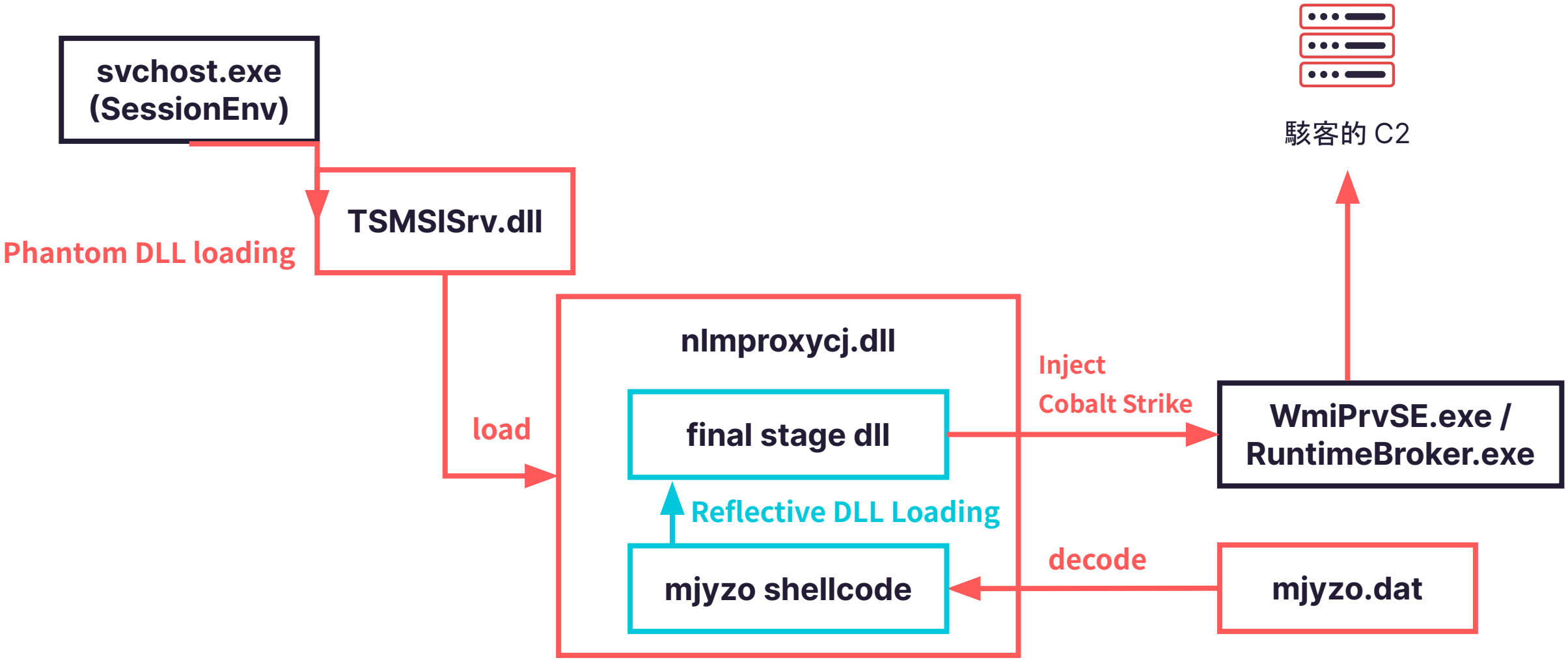
被動躲避 Sensors



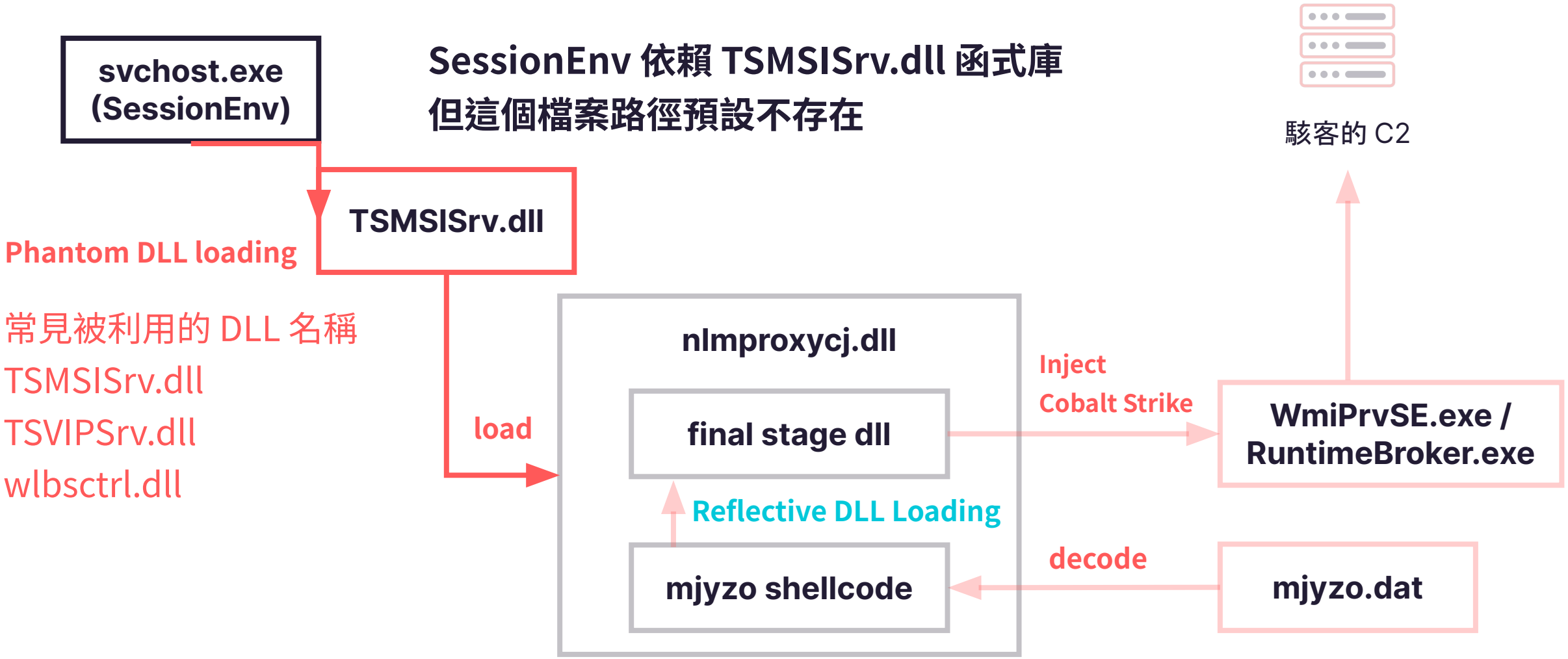
被動躲避 Sensors



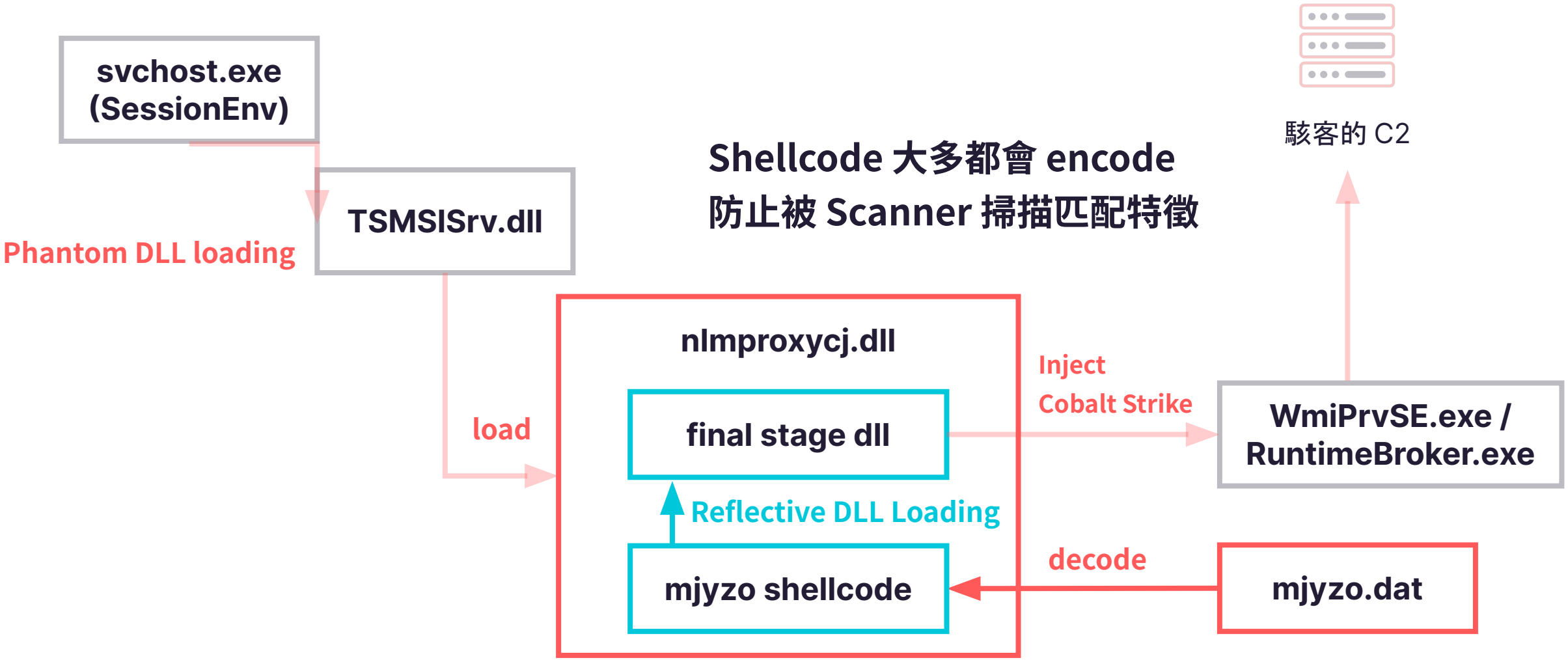
Multi-Stage Loader



Phantom DLL Loading

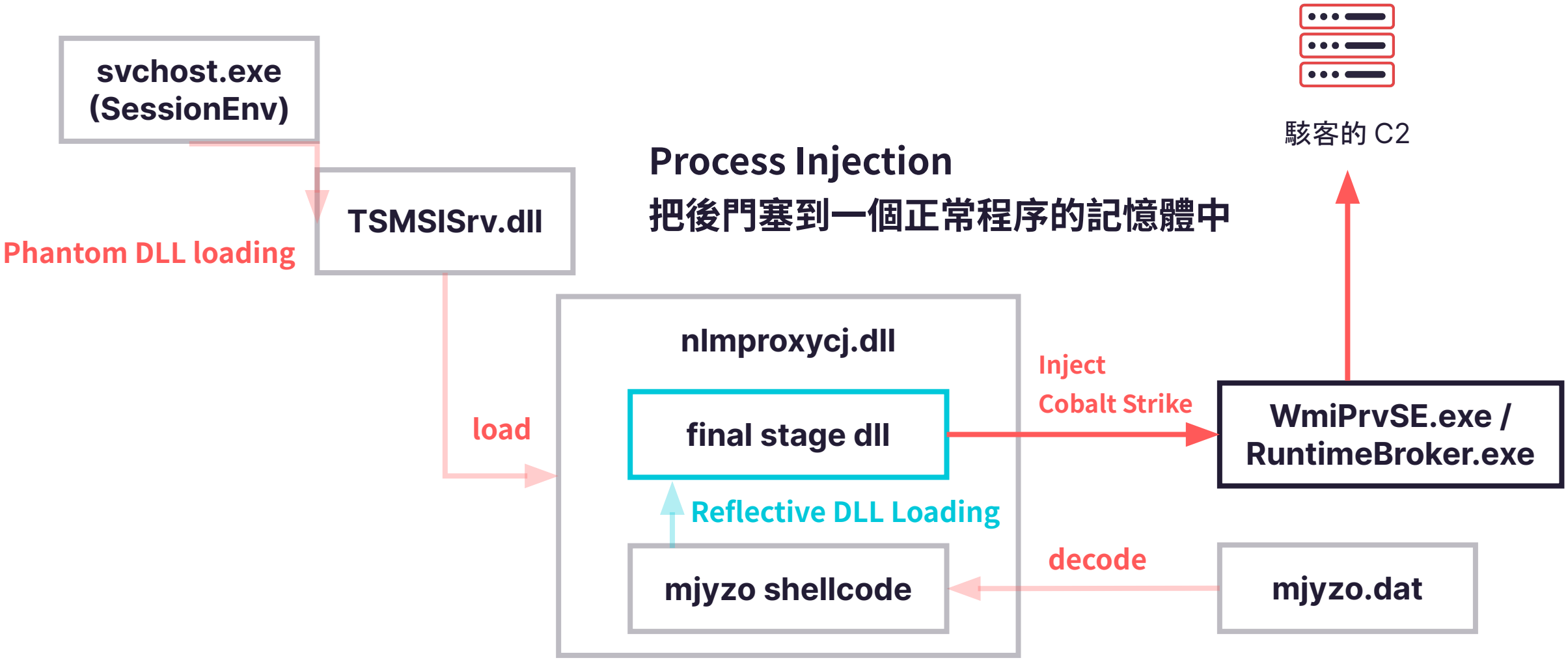


Decode Shellcode

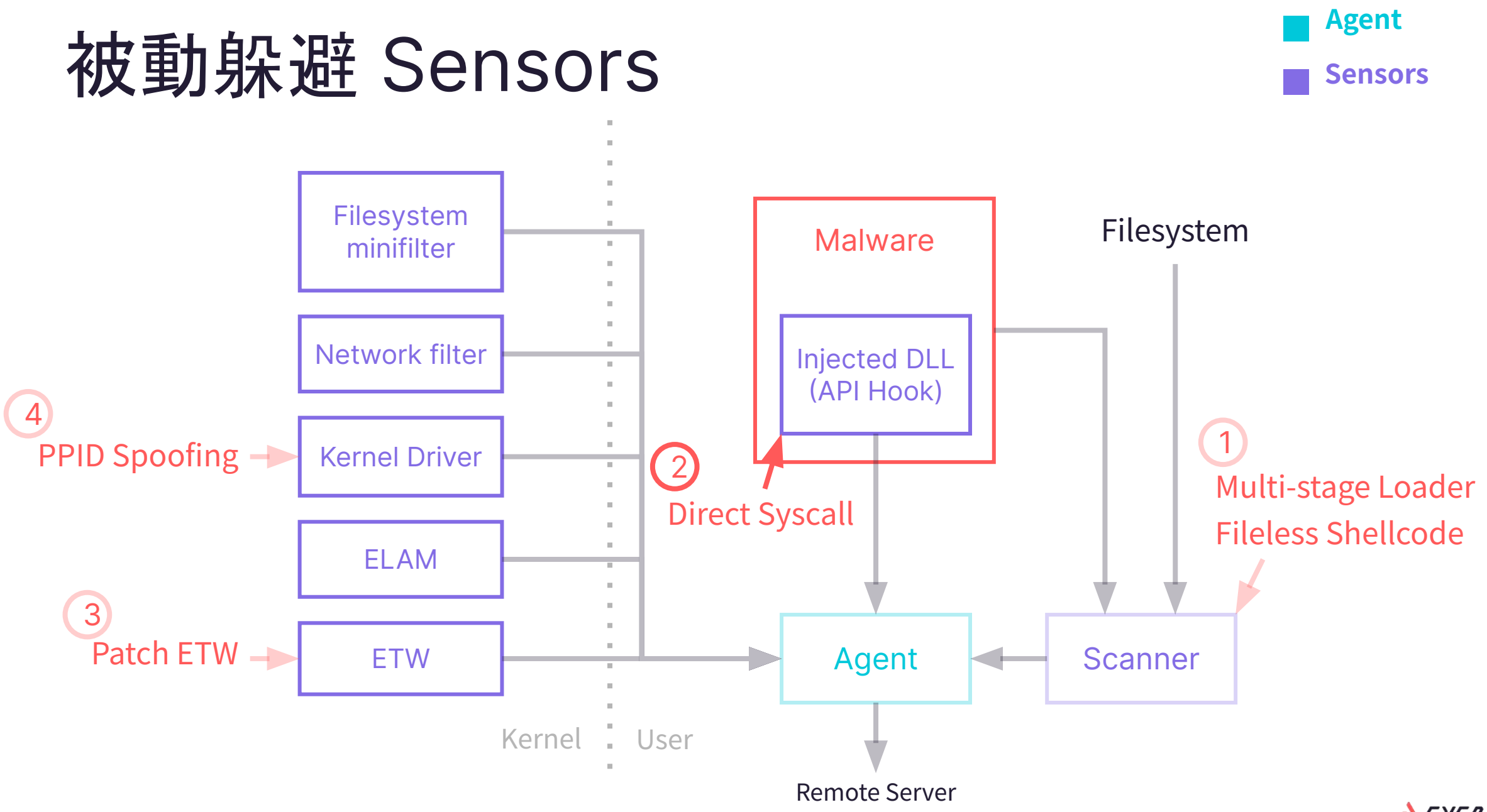


Shellcode 大多都會 encode
防止被 Scanner 掃描匹配特徵

Process Injection



被動躲避 Sensors



API Hooking

VirtualAllocEx

↓

WriteProcessMemory

↓

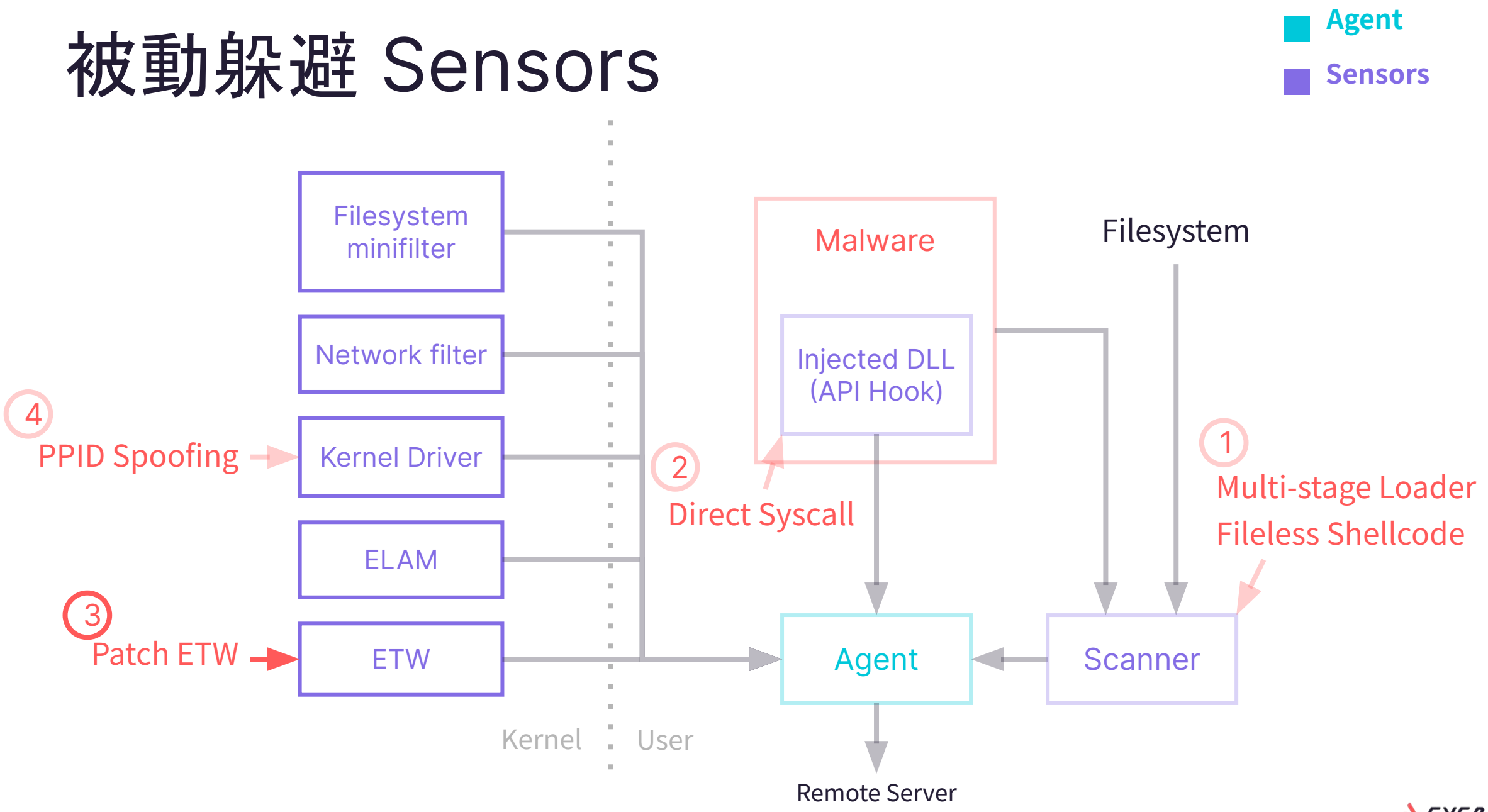
CreateRemoteThread

Direct Syscall

```
NTSTATUS __stdcall NtProtectVirtualMemory(
        HANDLE ProcessHandle,
        PVOID *BaseAddress,
        SIZE_T *NumberOfBytesToProtect,
        ULONG NewAccessProtection,
        PULONG OldAccessProtection)
{
  NTSTATUS result; // eax

  result = _sub_180004830_resolve_syscall_number_by_hash(0xB53FF1F);
  __asm { syscall; Low latency system call }
  return result;
}
```

被動躲避 Sensors

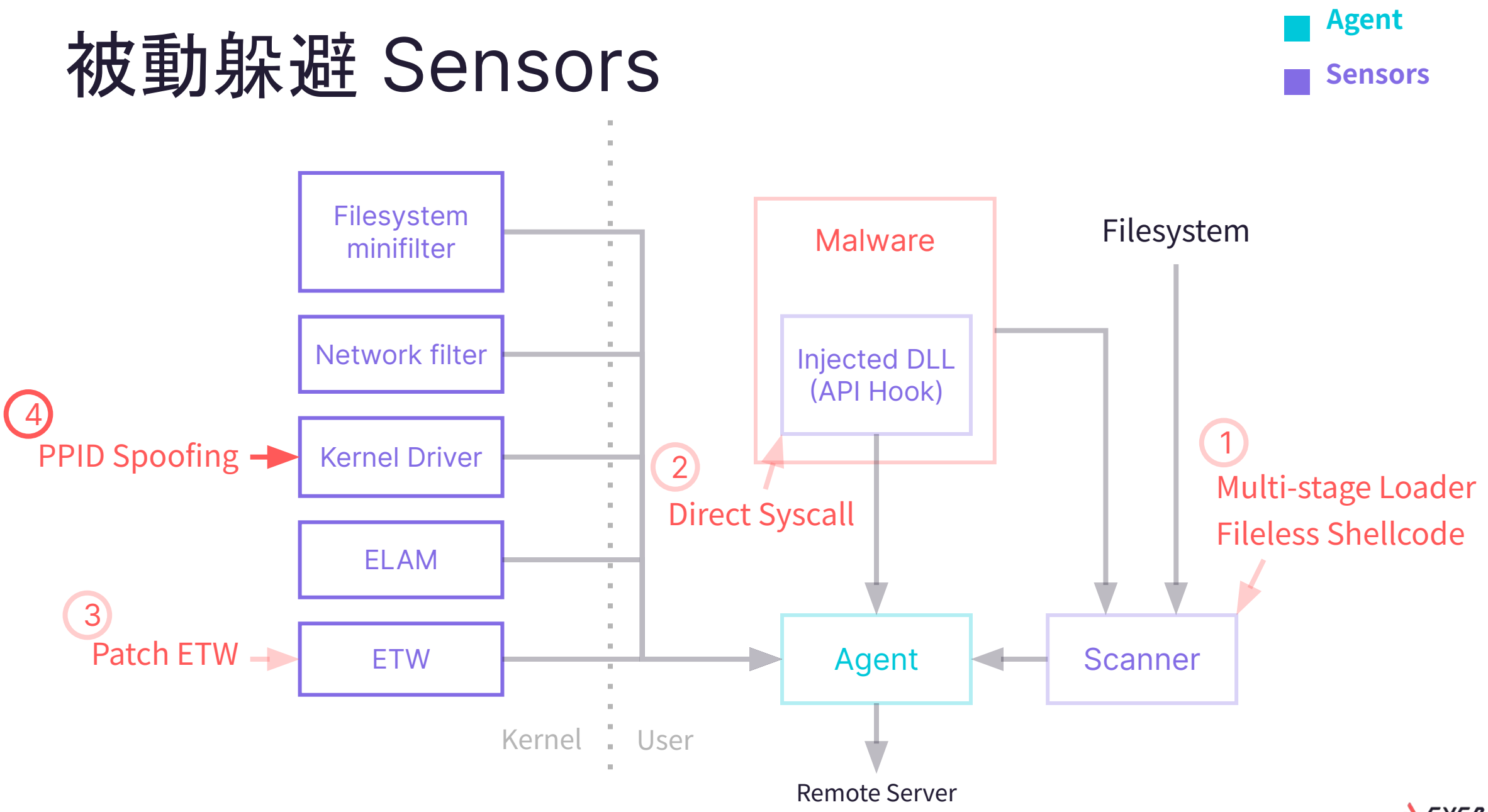


Hook EtwEventWrite

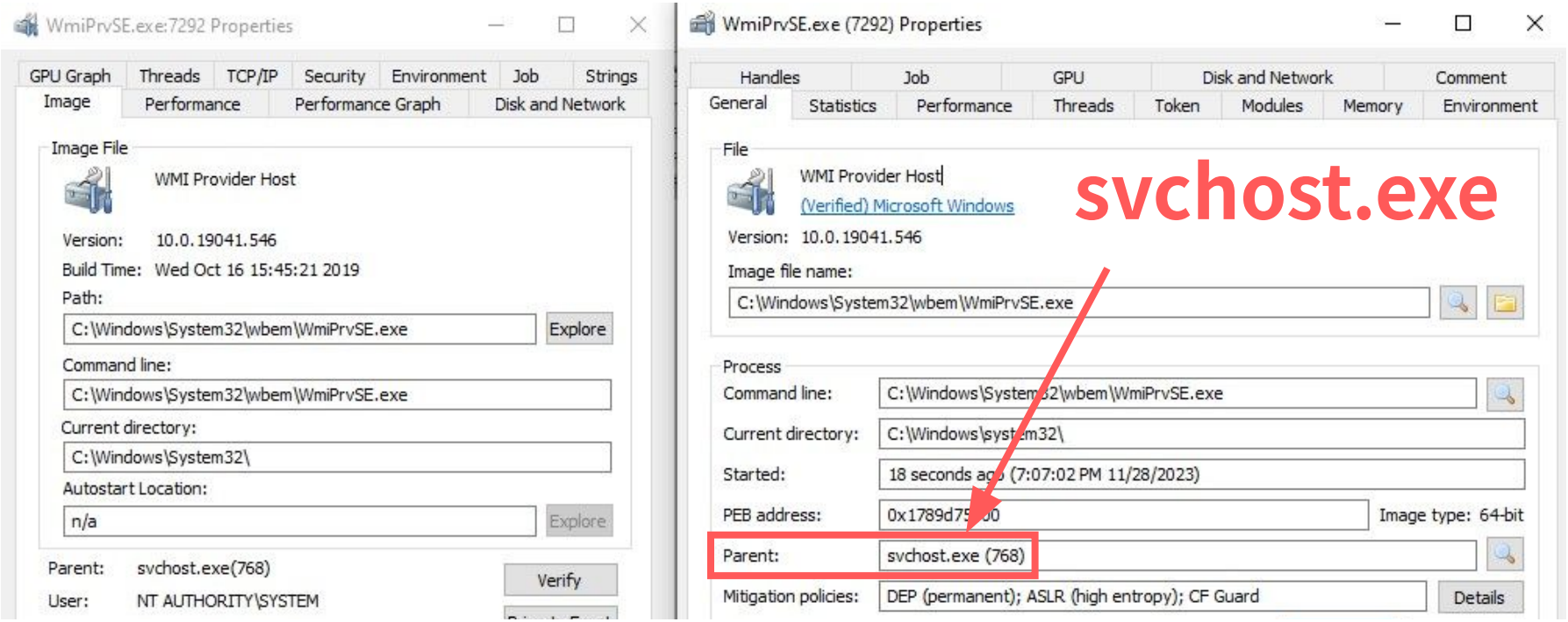
```
__int64 __fastcall _sub_180004B70_EtwEventWrite_Hook(__int64 a1, unsigned __int16 *a2, int a3, __int64 a4)
{
  int v5; // [rsp+40h] [rbp-28h]
  unsigned int v6; // [rsp+44h] [rbp-24h]
  unsigned int (__fastcall *EtwEventWriteFull)(__int64, unsigned __int16 *, _QWORD, _QWORD, _QWORD, int, __int64); // [rsp+48h] [rbp-20h]
  __int64 Library; // [rsp+50h] [rbp-18h]

  Library = _sub_180005080_LoadLibrary(0xDDB0C76F);
  EtwEventWriteFull = (unsigned int (__fastcall *)(__int64, unsigned __int16 *, _QWORD, _QWORD, _QWORD, int, __int64))_sub_180004F30_GetProcAddress(Library, 0x701D3D4F);
  v6 = 0;
  if ( !EtwEventWriteFull )
    return 1i64;
  v5 = *a2;
  if ( v5 != 0x58 && v5 != 0x8F && v5 != 0x9B )
    return EtwEventWriteFull(a1, a2, 0i64, 0i64, 0i64, a3, a4);
  return v6;
}
```

被動躲避 Sensors

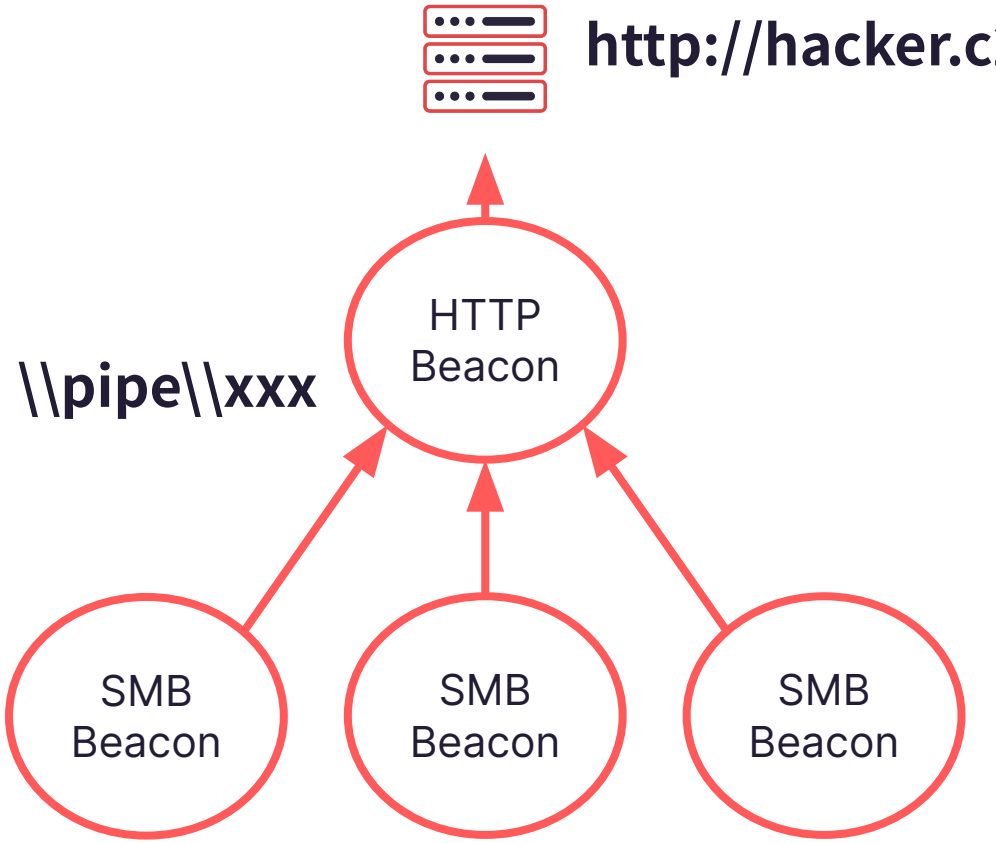


Parent PID Spoofing



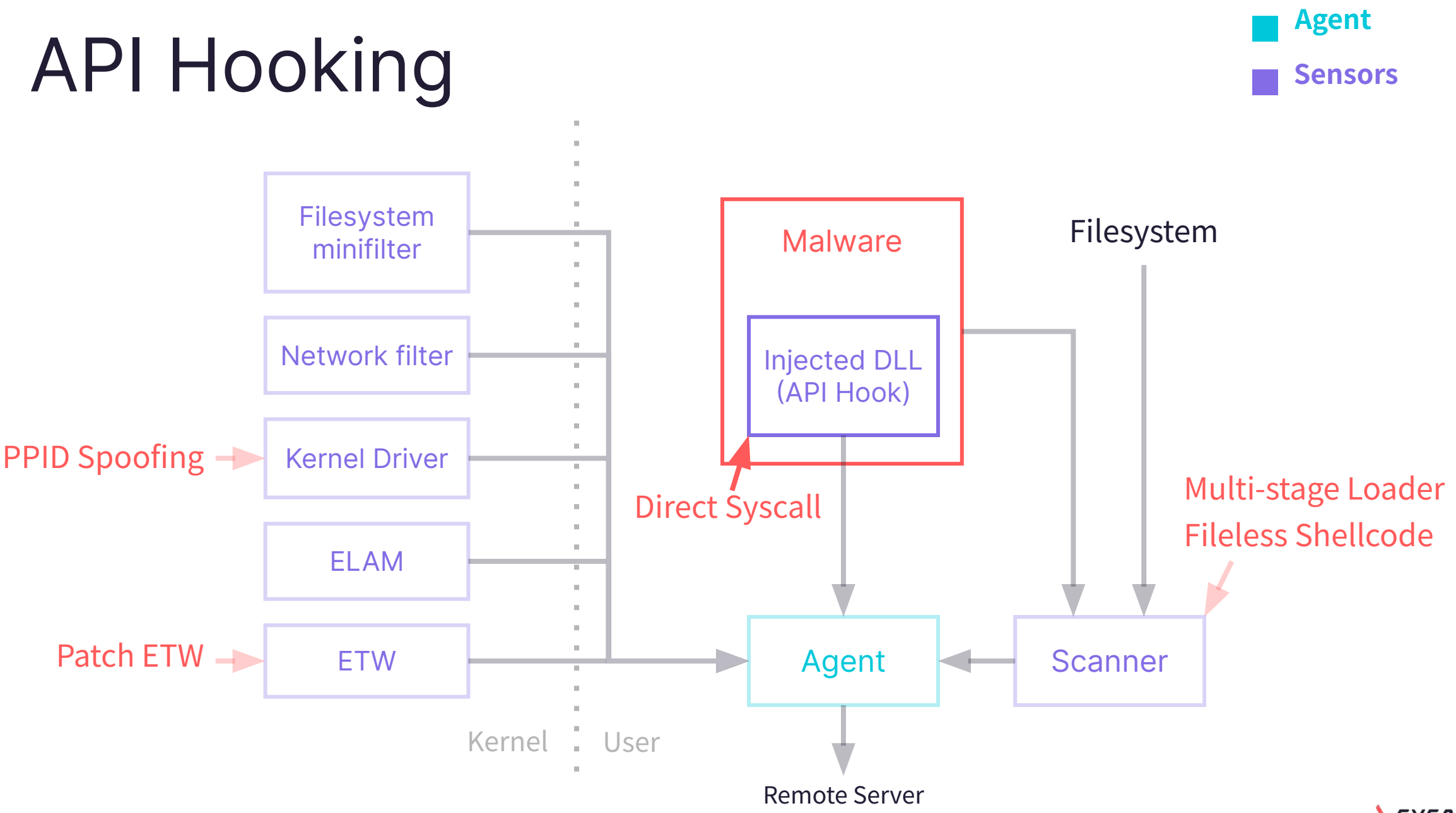
Cobalt Strike

```
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.119 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.39 >> \ipcsvc.6327.2791.721364981276491273623b
192.168.202.39 >> \ipcsvc.6327.2791.721364981276491273623b
```



Evasion 攻防戰

API Hooking



API Hooking

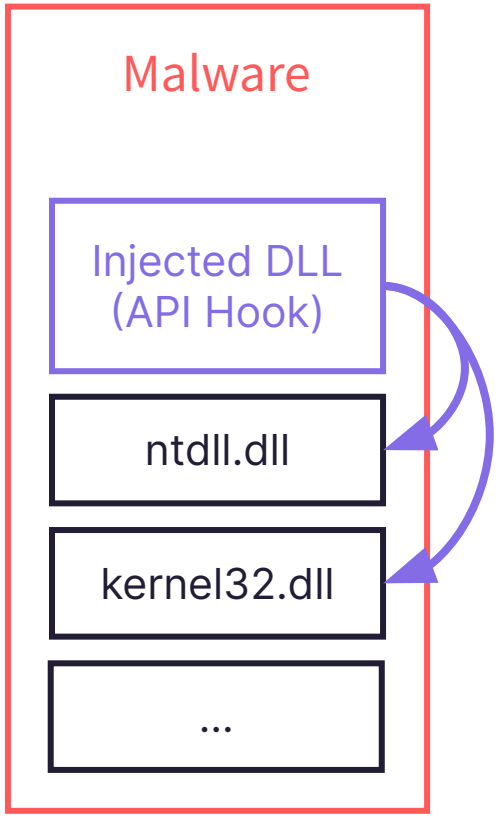
Before

TargetFunction:
  push ebp
  mov ebp, esp
  …

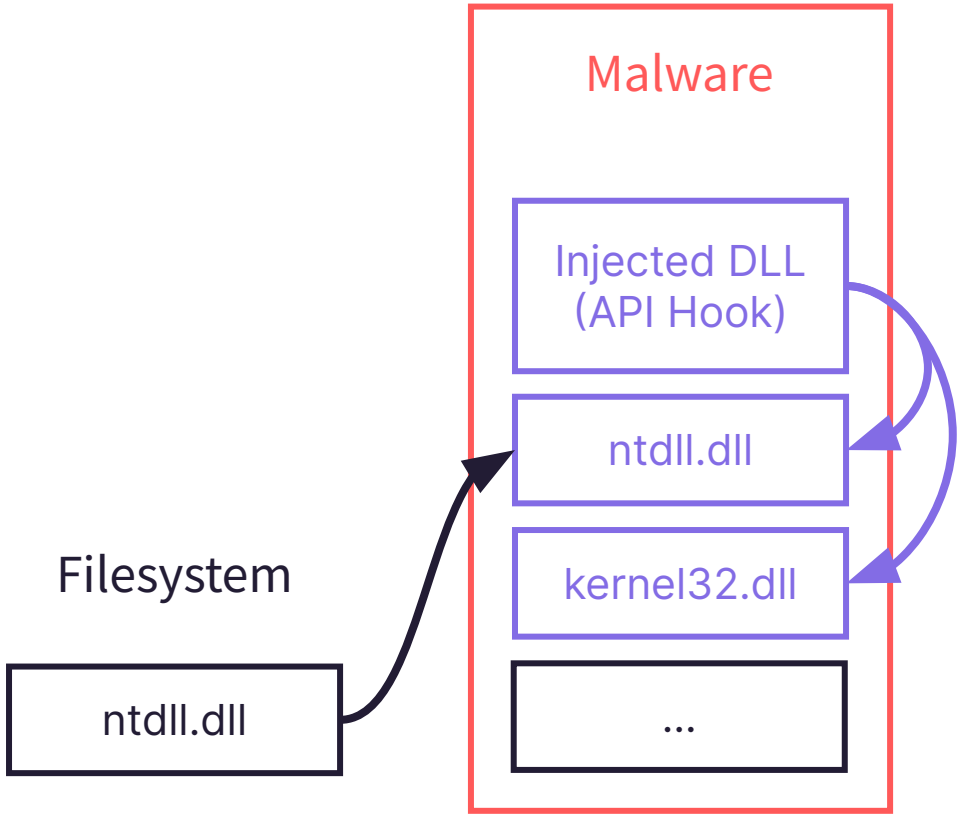
→

After

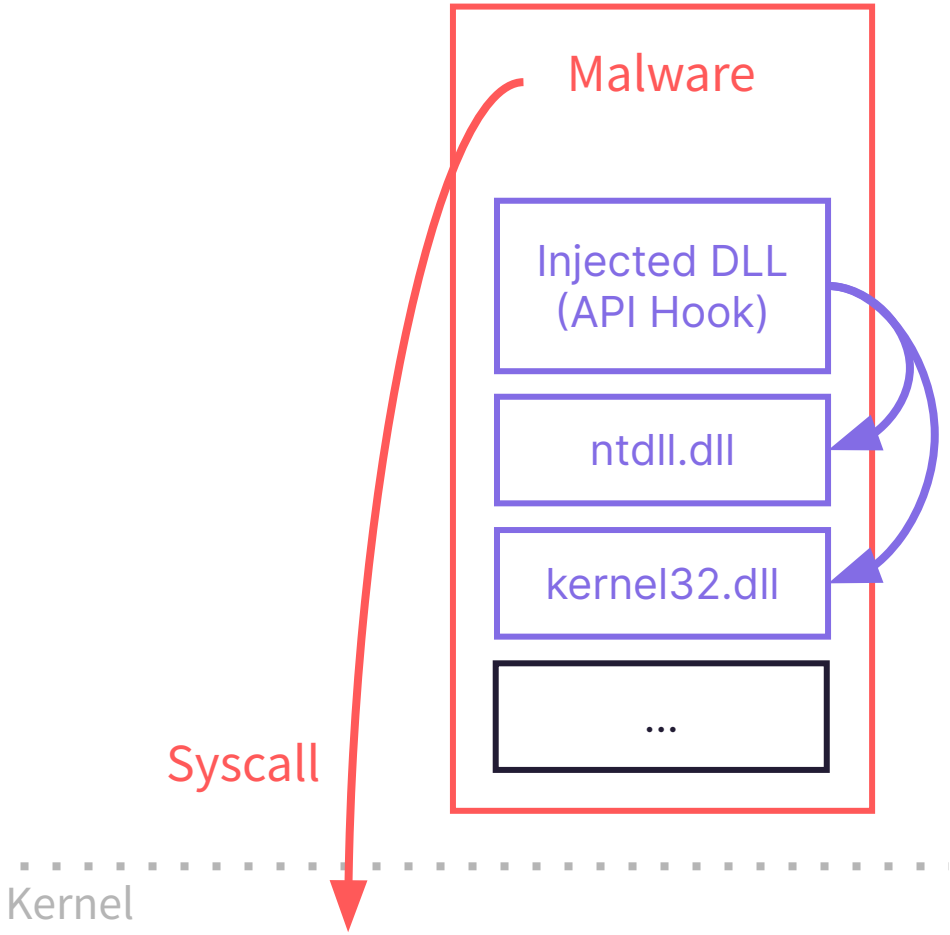
TargetFunction:
  jmp MyFunction
  …



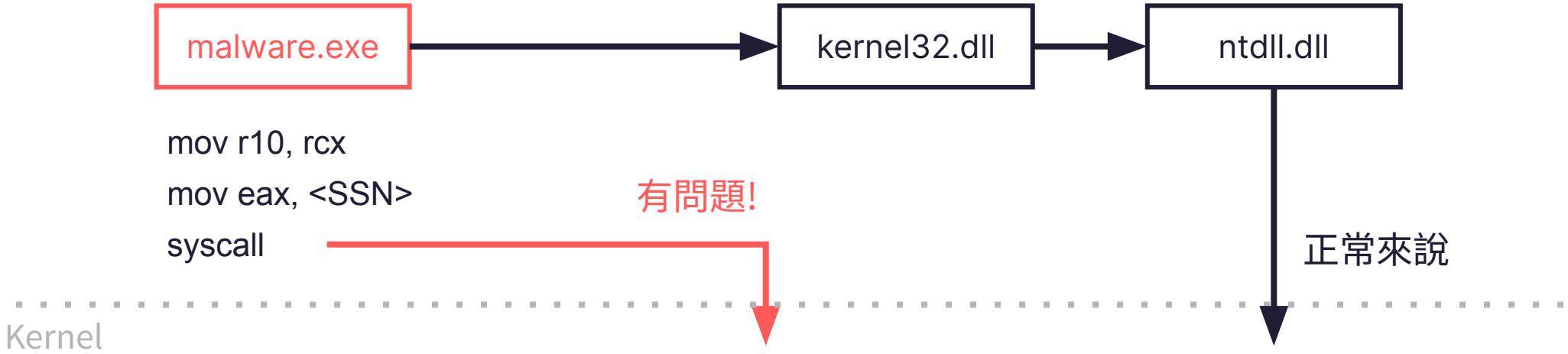
Evade API Hooking



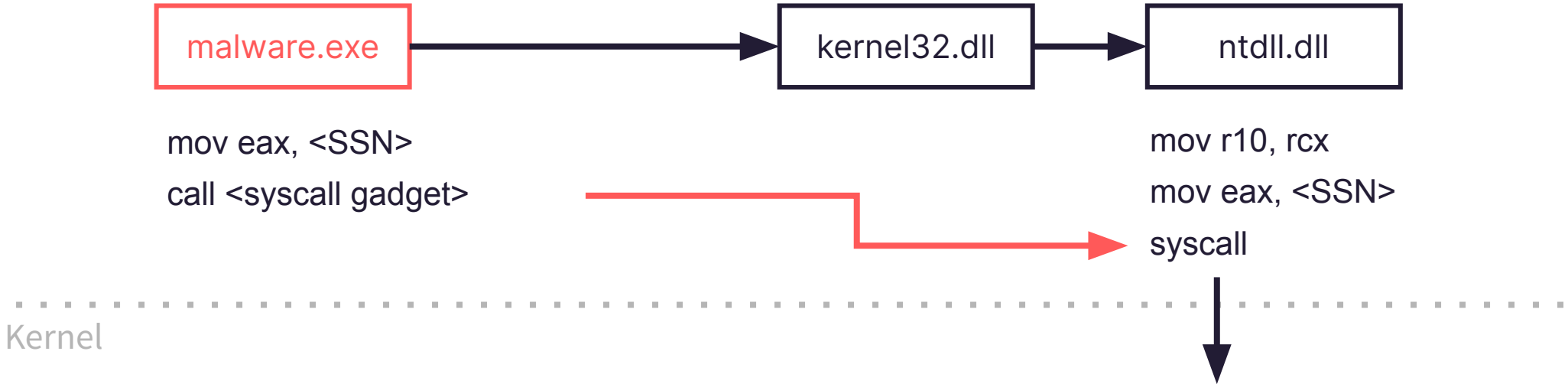
Evade API Hooking



Bypass Evade API Hooking

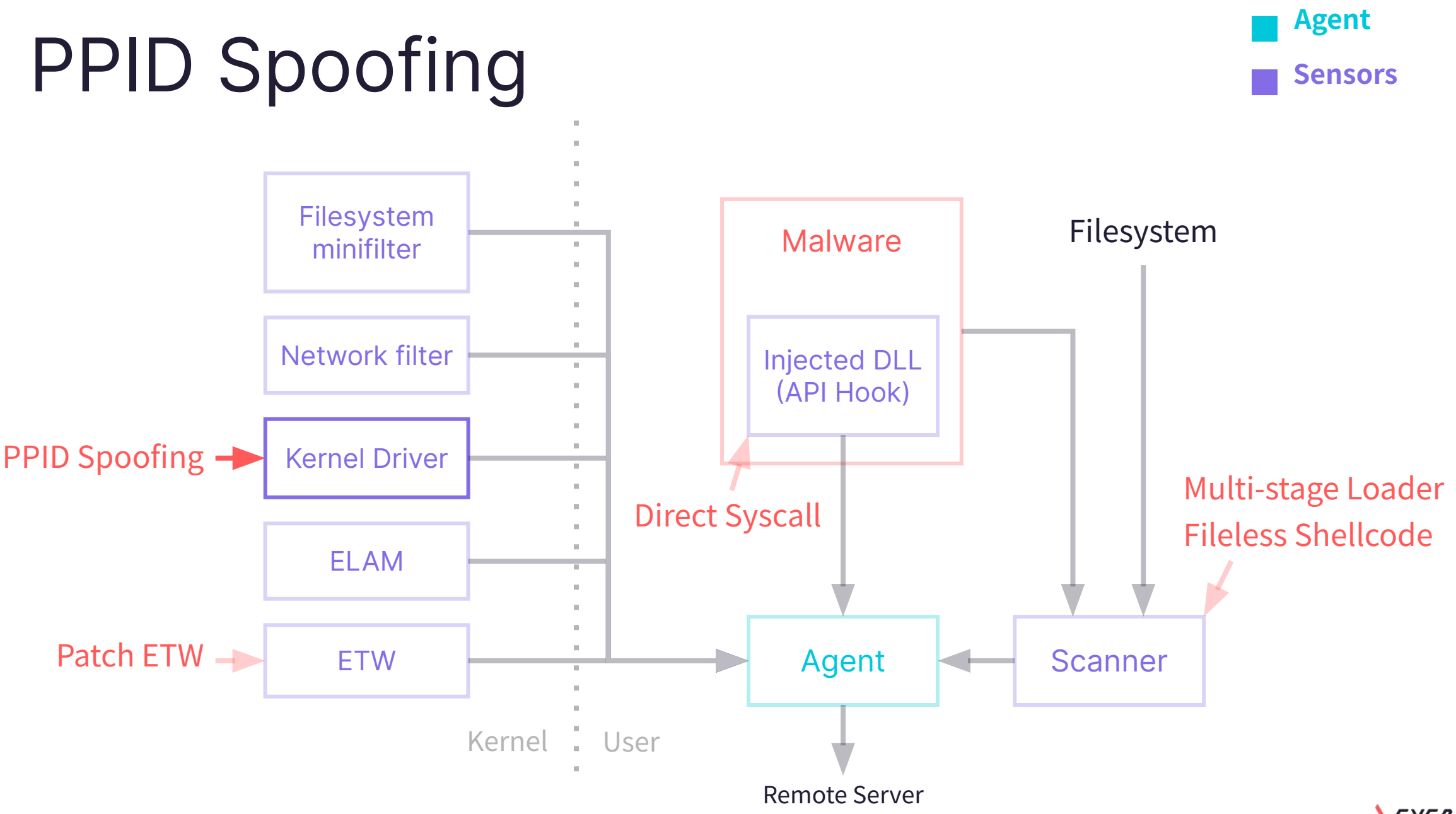


Evade Bypass Evade API Hooking



API Hooking 小結

PPID Spoofing



PPID Spoofing

Administrator: Windows Powe

```
PS C:\Users\jedi\Desktop> .\PPIDSpoofing.exe 672
TEB address: 000000227F748000
Original PID: 1764
Modified PID: 672
Press any key to continue...
```

svchost.exe	7080	2.63 MB	...\SYSTEM	Host Process fo...	System
svchost.exe	4236	1.66 MB	...\SYSTEM	Host Process fo...	System
svchost.exe	6440	2.69 MB	...\SYSTEM	Host Process fo...	System
TrustedInstaller.exe	7732	1.83 MB	...\SYSTEM	Windows Mod...	System
svchost.exe	7988	1.58 MB	...\SYSTEM	Host Process fo...	System
lsass.exe	672	5.55 MB	...\SYSTEM	Local Security ...	System
notepad.exe	8012	2.23 MB	DES...\jedi	Notepad	High
fontdrvhost.exe	808	1.44 MB	...\UMFD-(	Usermode Font...	Low

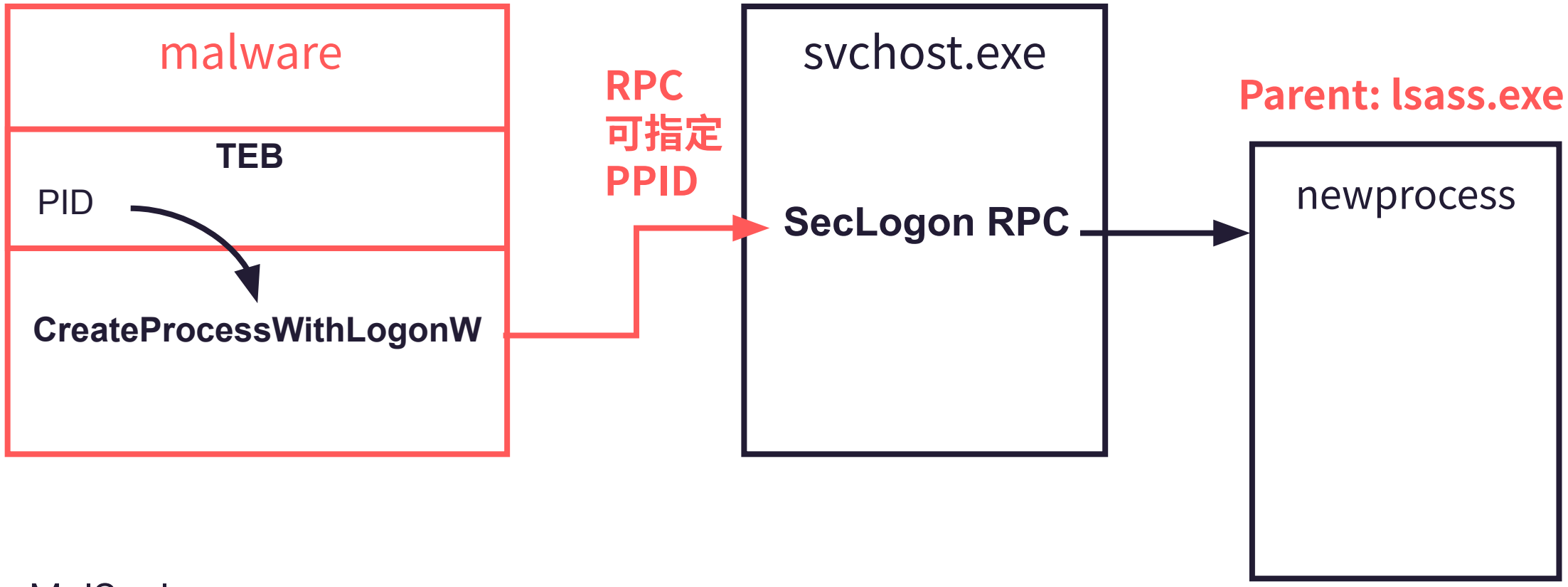
PPID Spoofing: 第一種作法

PROC_THREAD_ATTRIBUTE_PARENT_PROCESS	The *lpValue* parameter is a pointer to a handle to a process to use instead of the calling process as the parent for the process being created. The process to use must have the **PROCESS_CREATE_PROCESS** access right.

https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-updateprocthreadattribute

PPID Spoofing: 第二種作法

1. 改 TEB 上的 PID
2. 呼叫 CreateProcessWithLogonW



工具: MalSeclogon

https://splintercod3.blogspot.com/p/the-hidden-side-of-seclogon-part-2.html

Detect PPID Spoofing

Event 3, Kernel-Process

General | Details

Friendly View | XML View


```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-Kernel-Process" Guid="{22fb2cd6-0e7b-422b-a0c7-2fad1fd0e716}" />
      <EventID>3</EventID>
      <Version>1</Version>
      <Level>4</Level>
      <Task>3</Task>
      <Opcode>1</Opcode>
      <Keywords>0x8000000000000020</Keywords>
      <TimeCreated SystemTime="2024-04-25T10:02:27.4539060Z" />
      <EventRecordID>35</EventRecordID>
      <Correlation />
      <Execution ProcessID="416" ThreadID="5012" />
      <Channel />
      <Computer>DESKTOP-SJHOB97</Computer>
      <Security />
    </System>
```

Takeaway

- 防止 BYOVD，可以把常被利用的驅動加入黑名單
- Direct Syscall 目前主流 Bypass API Hooking 手法，有 syscall 的程式通常有問題
- Parent Process 不一定等於 Process Creator

奧義 AI 資安年會

CRAFTCON TAIWAN

台灣首場資安為主題的 AI 技術研討會

2024.07.12 (五) 08:30 - 17:00

資料科學研發處長 楊政霖 博士

創辦人 邱銘彰 (Birdman)

資安研究處長 陳仲寬

格萊天漾大飯店 艋舺廳 (台灣台北市萬華區艋舺大道101號14樓)

CYCRAFT 奧義智慧科技