潛入核心：
惡意程式與驅動程式的狼狽為奸

TeamT5 Engine Team－Zeze

TEAMT5
杜 浦 數 位 安 全
Persistent Cyber Threat Hunters

TEAMT5
杜 浦 數 位 安 全

Zeze

- TeamT5 資安研究員
- BambooFox、⚔️TSJ⚔️ 戰隊隊員
- HITCON 2022、VXCON 2022 講者
- 40+ Windows Kernel CVEs

Outline

TEAMT5
杜 浦 數 位 安 全

01 BYOVD 攻擊

02 漏洞利用

03 攻擊目的

04 案例分析

05 改善與防禦

BYOVD 攻擊

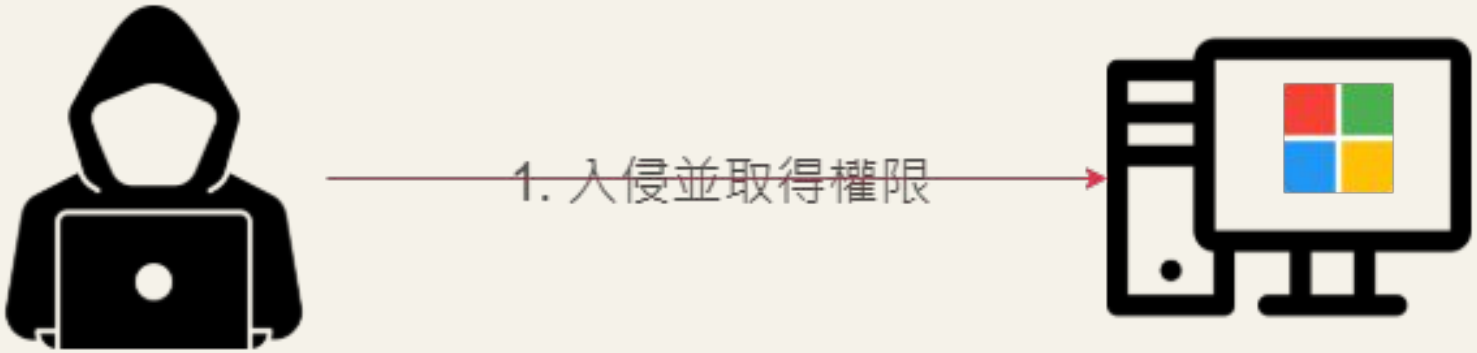
BYOVD 簡介

簡單介紹 BYOVD 攻擊

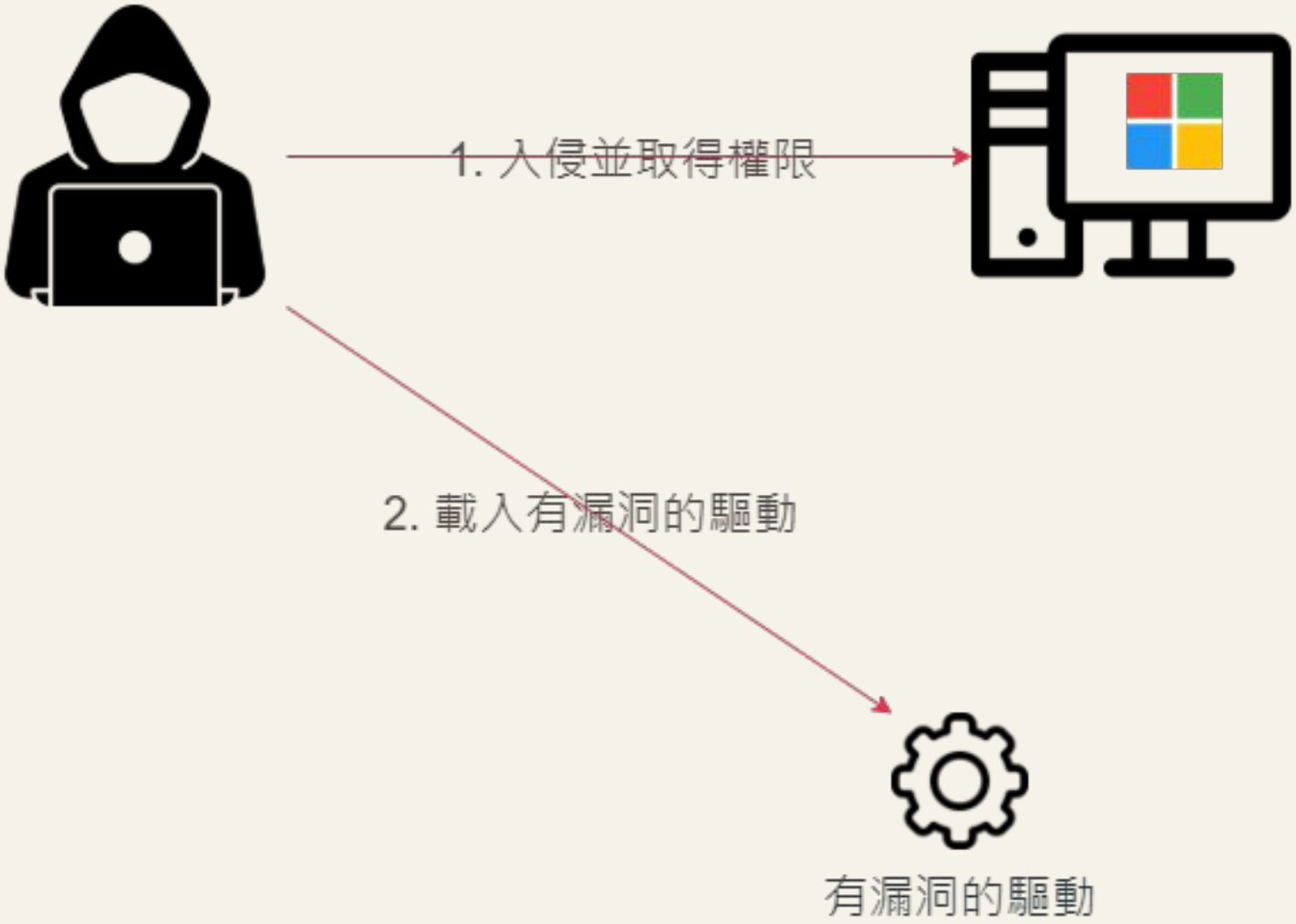
BYOVD (Bring Your Own Vulnerable Driver) 攻擊是一種針對作業系統的攻擊，利用作業系統允許使用者自行安裝驅動程序的特性。攻擊者可以在作業系統中**安裝一個有漏洞的驅動程式**，透過驅動程式的漏洞來**取得核心執行權限**或者進行其他的攻擊。在 BYOVD 攻擊中，攻擊者通常會尋找已知的漏洞或者利用新發現的漏洞來開發自己的漏洞利用程式。

- ChatGPT

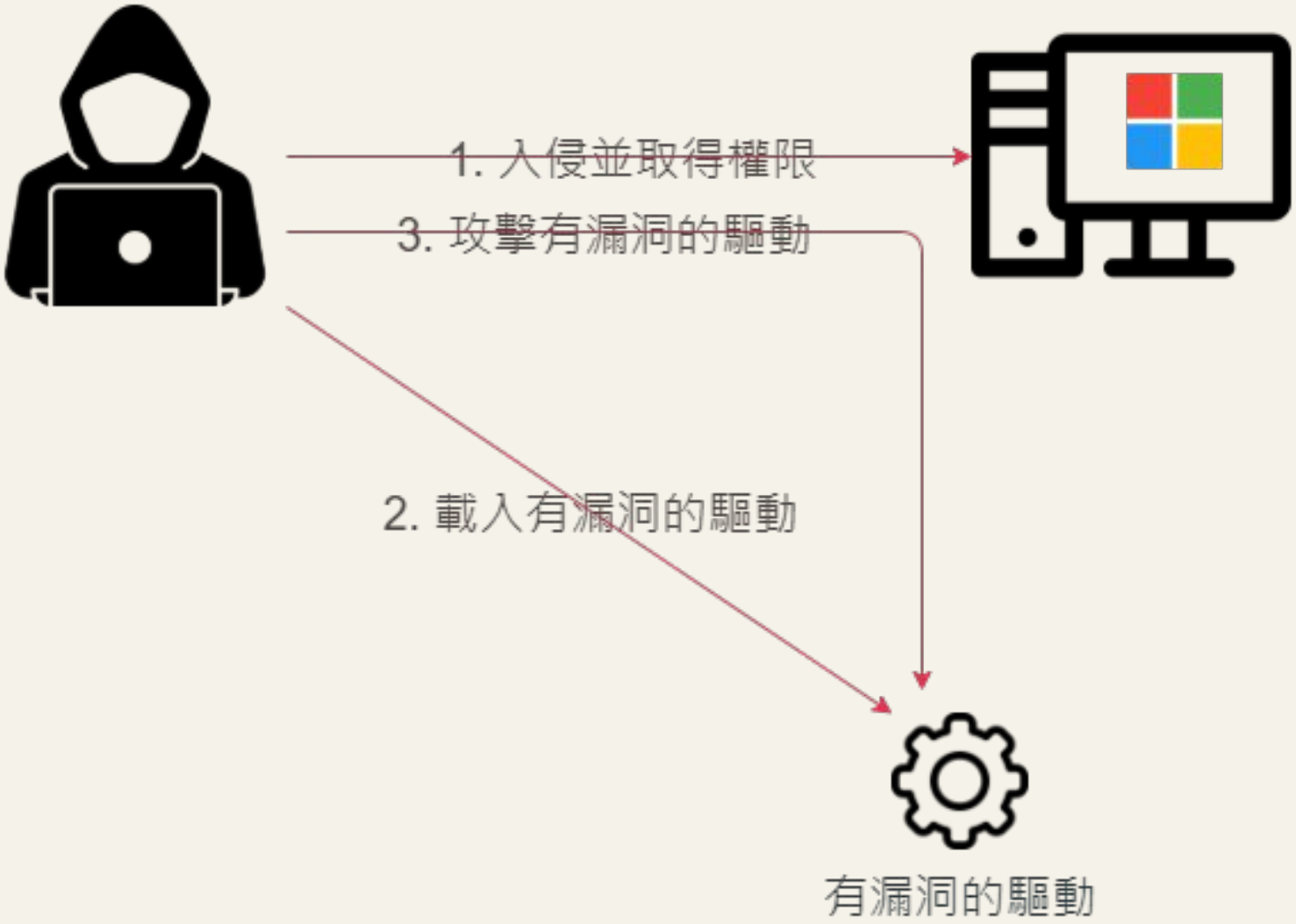
BYOVD 攻擊示意圖



BYOVD 攻擊示意圖

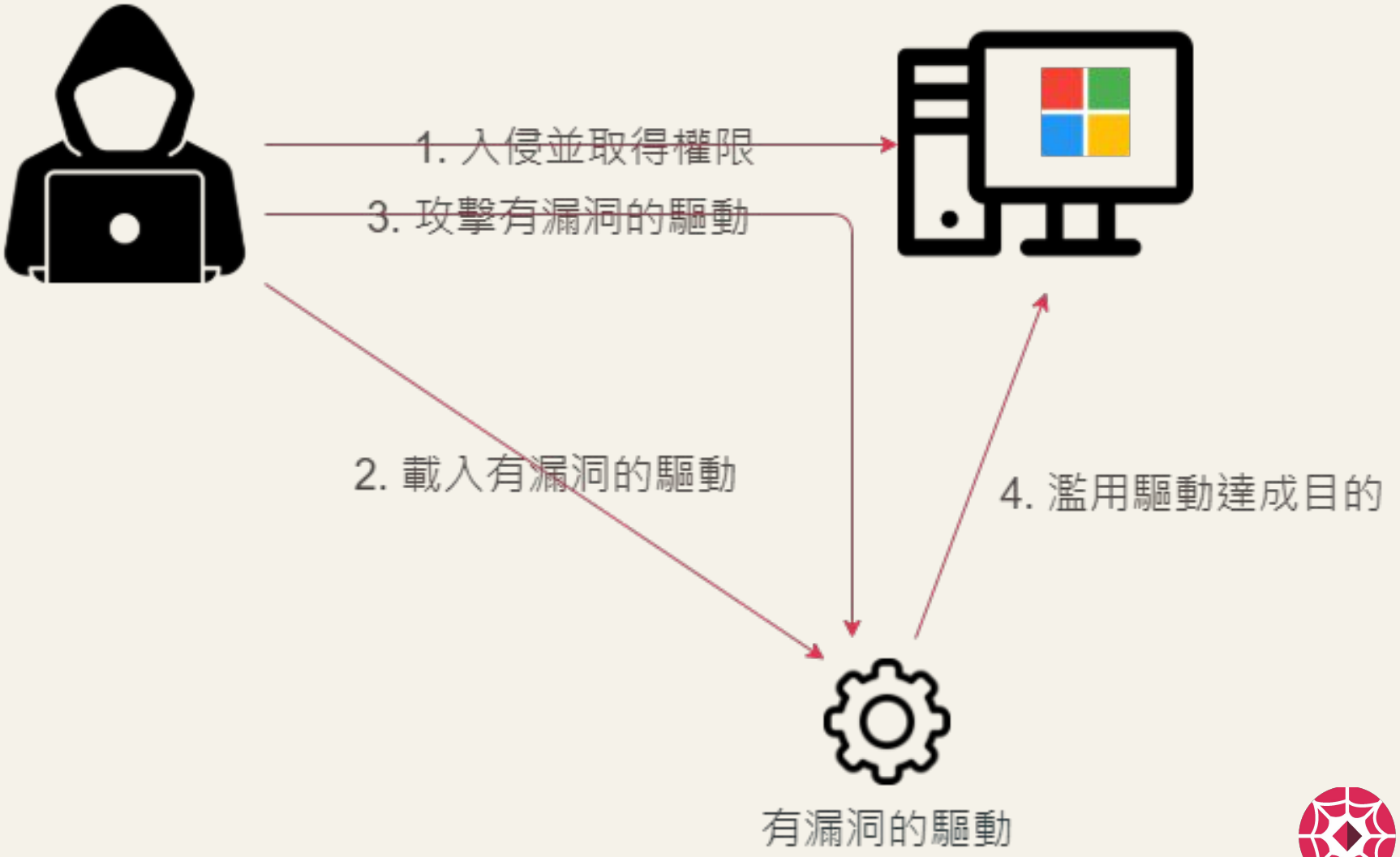


BYOVD 攻擊示意圖



TEAMT5
杜 浦 數 位 安 全

BYOVD 攻擊示意圖



TEAMT5
杜 浦 數 位 安 全

Driver Signing

簡單解釋 Windows 的 Driver Signing

Windows 的 Driver Signing 是一種保證驅動程式的安全和可靠性的機制。**驅動程式需要經過簽章才能在 Windows 上執行**。驅動程式簽名檢驗的過程將會驗證驅動程式的簽章，以確保驅動程式的安全和可靠性。如果驅動程式沒有經過簽章，或者簽章失敗，則 Windows 將會拒絕載入驅動程式。

- ChatGPT

漏洞利用

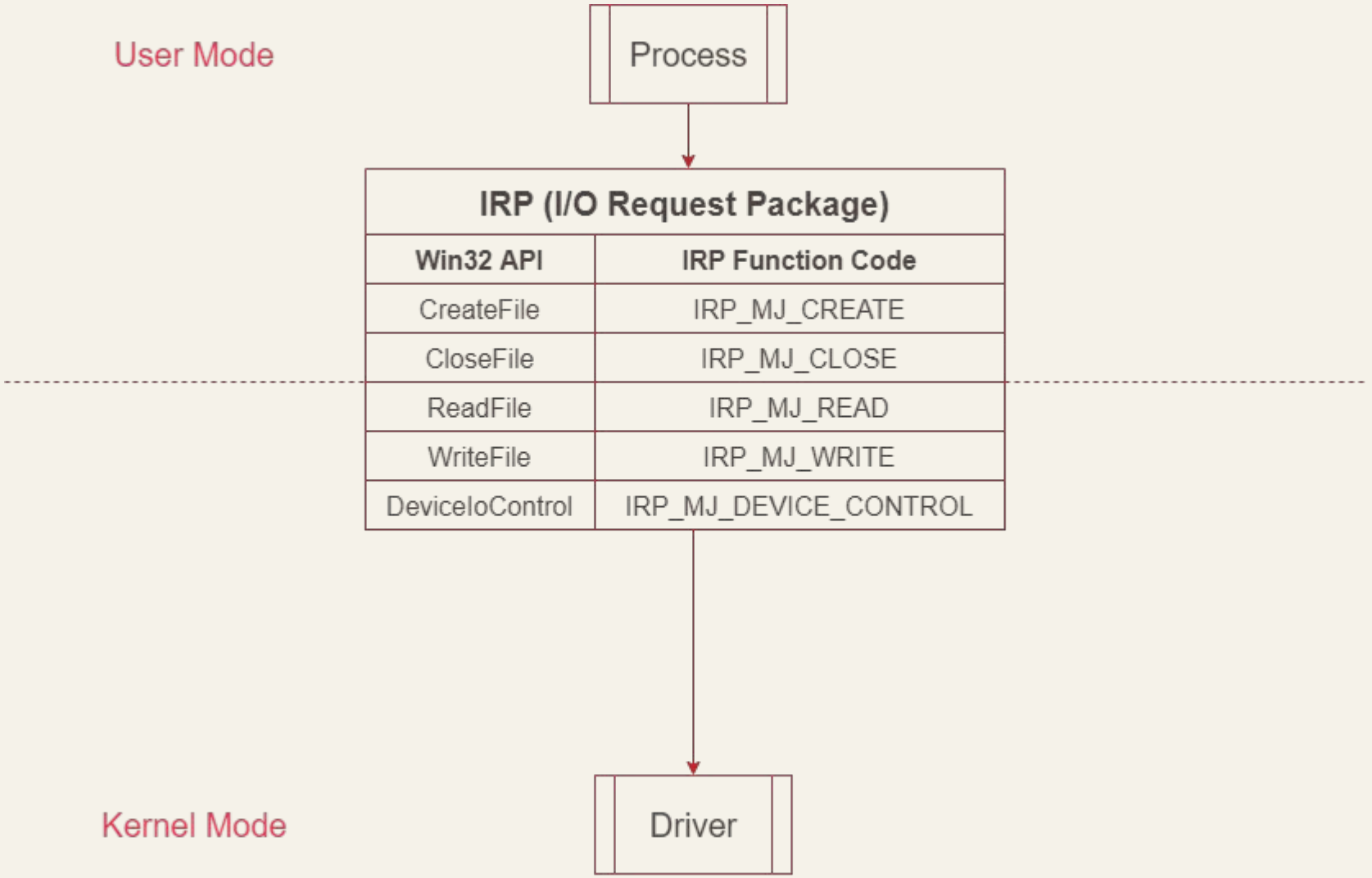
IRP

簡單解釋 Windows 的 IRP

IRP (I/O Request Packet) 是 **Windows 系統中用於請求 I/O 操作的資料結構**。在 Windows 中，驅動程序可以**使用 IRP 來與系統核心溝通**，以實現 I/O 操作，例如讀取磁盤上的文件或向網絡進行數據傳輸。IRP 包含了關於請求的詳細信息，包括操作種類、操作的數據等。驅動程式可以提交 IRP 給 I/O 管理器，它將負責將 IRP 轉發給相應的驅動程序。

- ChatGPT

IRP 示意圖



常見被利用漏洞類型

- 任意讀寫 kernel memory
- 任意讀寫 physical memory
- 參數可控的 writemsr
- 任意執行 shellcode

任意讀寫 Kernel Memory 範例

```
*(CHAR *)UserInput = *(CHAR *)(UserInput + 4);
```

例 1. 對任意位址寫入任意值

```
memcpy((CHAR *)UserInput, (CHAR *)(UserInput + 4), 4)
```

例 2. memcpy 的 dest、src 可控

任意讀寫 Kernel Memory 範例

```
*(CHAR *)UserInput = *(CHAR *)(UserInput + 4);
```

例 1. 對任意位址寫入任意值

```
memcpy((CHAR *)UserInput, (CHAR *)(UserInput + 4), 4)
```

例 2. memcpy 的 dest、src 可控

```
void *memcpy (
    void *dest,
    const void *src,
    size_t count
);
```

TEAMT5
杜 浦 數 位 安 全

任意讀寫 Physical Memory 範例

```
PhysicalMemory = MmMapIoSpace(*(PHYSICAL_ADDRESS *)UserInput, *(SIZE_T *)(UserInput + 8), MmNonCached);

*(CHAR *)PhysicalMemory = *(CHAR *)(UserInput + 12);
```

例 1. 參數可控的 MmMapIoSpace

```
ZwMapViewOfSection(
    *(HANDLE *)UserInput,
    *(HANDLE *)(UserInput + 8),
    *(PVOID **)(UserInput + 16),
    0,
    0,
    NULL,
    &viewSize,
    ViewShare,
    0,
    PAGE_READONLY
);
```

例 2. 參數可控的 ZwMapViewOfSection

任意讀寫 Physical Memory 範例

```
PhysicalMemory = MmMapIoSpace(*(PHYSICAL_ADDRESS *)UserInput, *(SIZE_T *)(UserInput + 8), MmNonCached);

*(CHAR *)PhysicalMemory = *(CHAR *)(UserInput + 12);
```

例 1. 參數可控的 MmMapIoSpace

```
PVOID MmMapIoSpace (
    PHYSICAL_ADDRESS    PhysicalAddress,
    SIZE_T              NumberOfBytes,
    MEMORY_CACHING_TYPE CacheType
);
```

```
ZwMapViewOfSection(
    *(HANDLE *)UserInput,
    *(HANDLE *)(UserInput + 8),
    *(PVOID **)(UserInput + 16),
    0,
    0,
    NULL,
    &viewSize,
    ViewShare,
    0,
    PAGE_READONLY
);
```

例 2. 參數可控的 ZwMapViewOfSection

TEAMT5 杜浦數位安全

任意讀寫 Physical Memory 範例

```
PhysicalMemory = MmMapIoSpace(*(PHYSICAL_ADDRESS *)UserInput, *(SIZE_T *)(UserInput + 8), MmNonCached);

*(CHAR *)PhysicalMemory = *(CHAR *)(UserInput + 12);
```

例 1. 參數可控的 MmMapIoSpace

```
ZwMapViewOfSection(
    *(HANDLE *)UserInput,
    *(HANDLE *)(UserInput + 8),
    *(PVOID **)(UserInput + 16),
    0,
    0,
    NULL,
    &viewSize,
    ViewShare,
    0,
    PAGE_READONLY
);
```

```
NTSYSAPI NTSTATUS ZwMapViewOfSection (
      HANDLE          SectionHandle,
      HANDLE          ProcessHandle,
      PVOID           *BaseAddress,
      ULONG_PTR       ZeroBits,
      SIZE_T          CommitSize,
      PLARGE_INTEGER  SectionOffset,
      PSIZE_T         ViewSize,
      SECTION_INHERIT InheritDisposition,
      ULONG           AllocationType,
      ULONG           Win32Protect
);
```

例 2. 參數可控的 ZwMapViewOfSection

參數可控的 writemsr

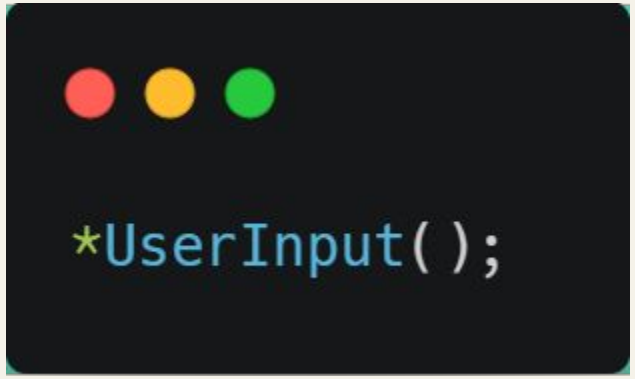
```
__writemsr(*(int *)UserInput, *(unsigned long long *)(UserInput + 8));
```

例. 參數可控的 writemsr

```
void __writemsr (
    unsigned long Register,
    unsigned __int64 Value
);
```

TEAMT5
杜 浦 數 位 安 全

任意執行 Shellcode



例. 直接執行使用者的輸入

攻擊目的

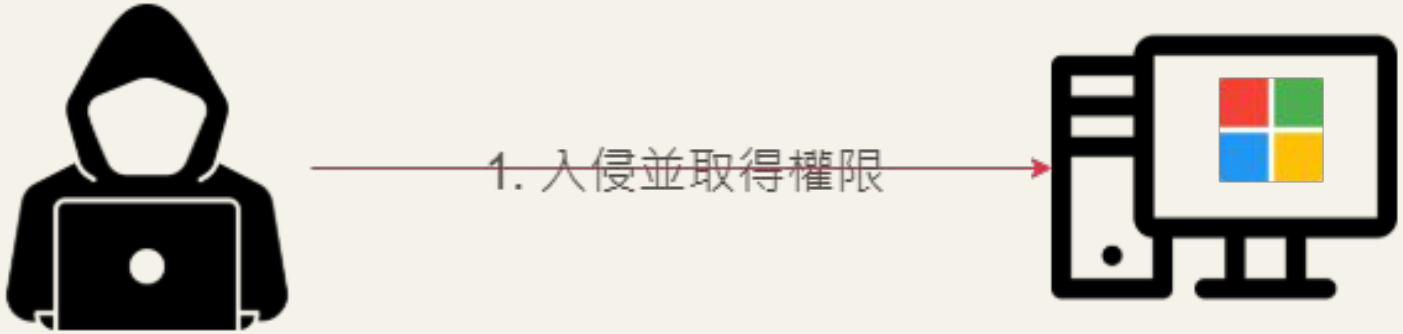
BYOVD 的目的

- 攻擊防毒軟體
- 埋後門
- 隱藏蹤跡
- 破壞系統

BYOVD 的目的

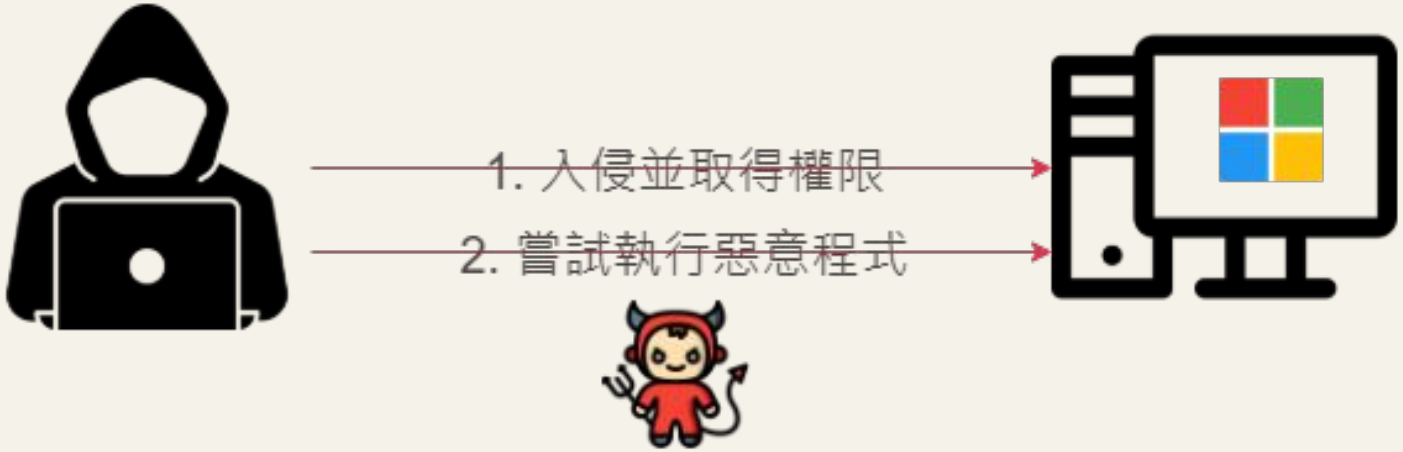
- **攻擊防毒軟體**
- 埋後門
- 隱藏蹤跡
- 破壞系統

攻擊防毒軟體——一般情況



防毒軟體

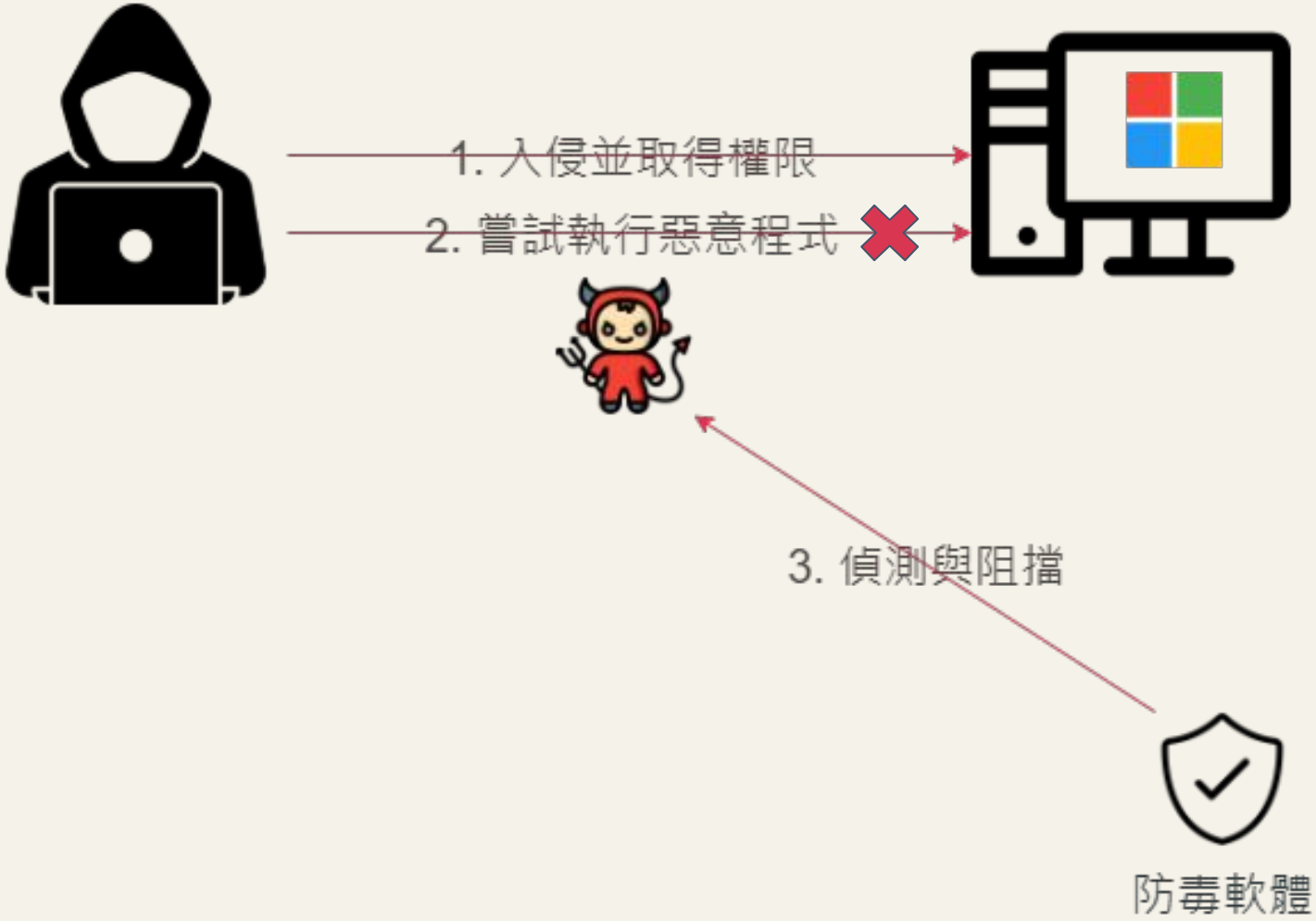
攻擊防毒軟體——一般情況



防毒軟體

攻擊防毒軟體——一般情況

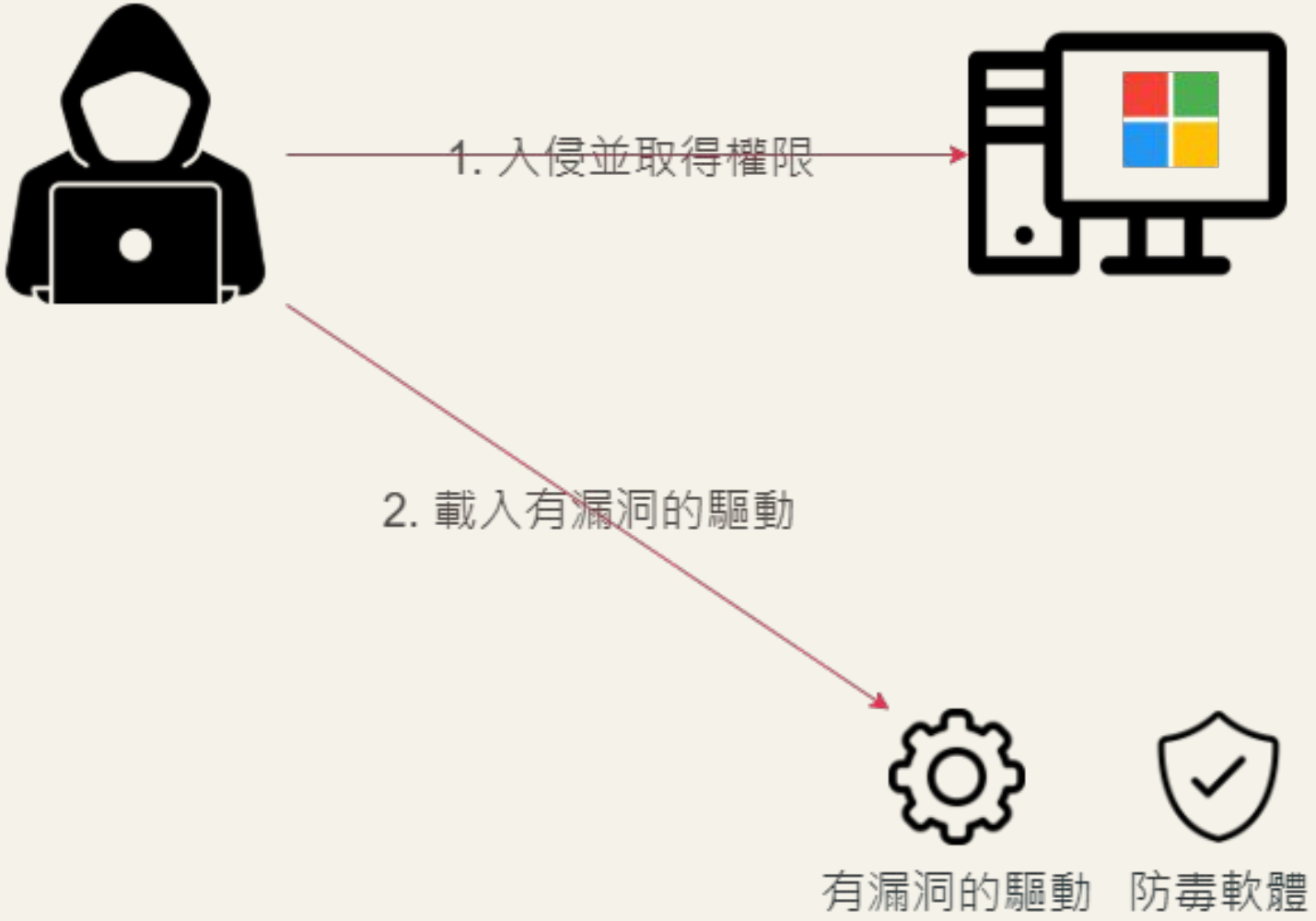
TEAMT5
杜 浦 數 位 安 全



攻擊防毒軟體－BYOVD

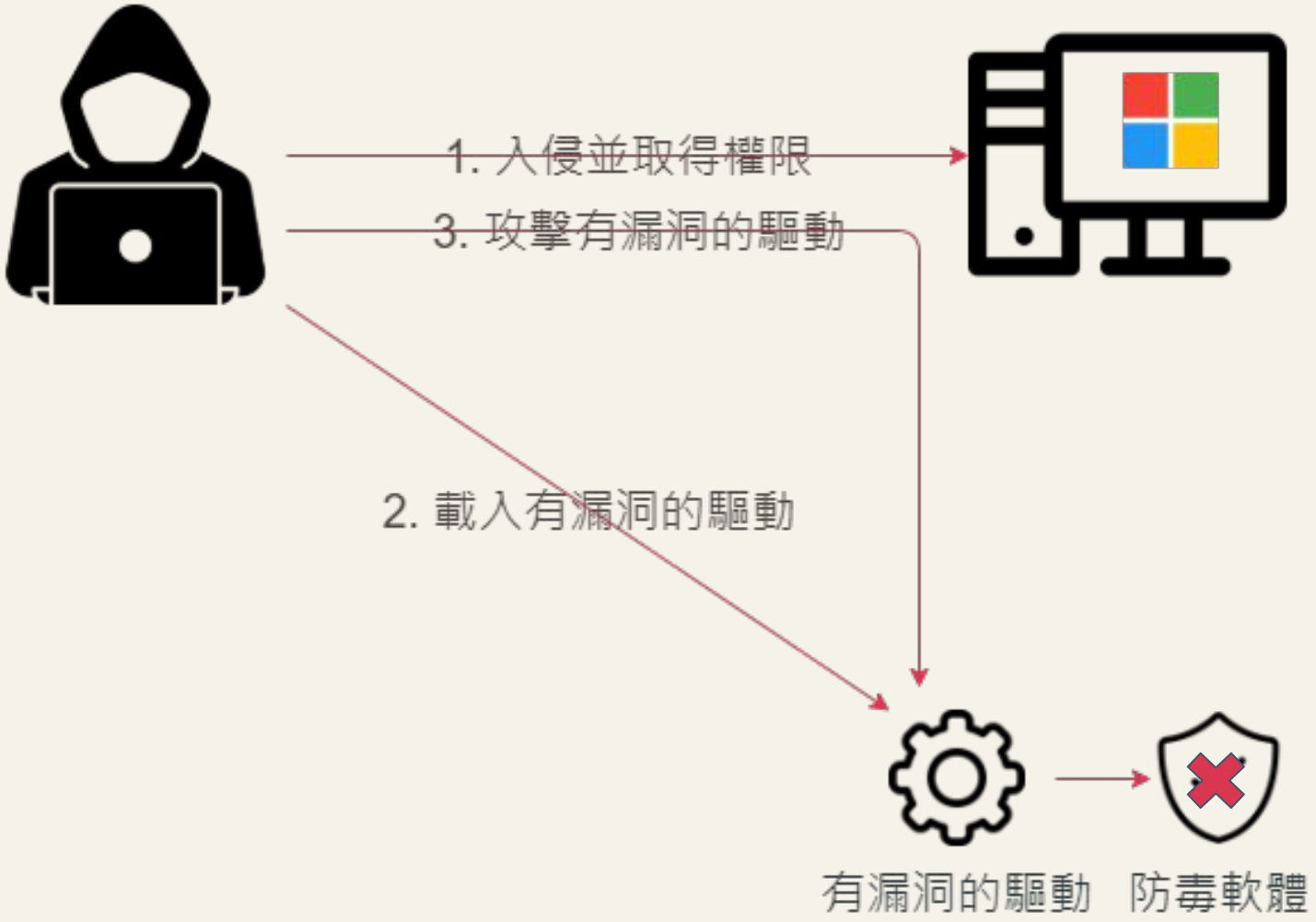
防毒軟體

攻擊防毒軟體－BYOVD



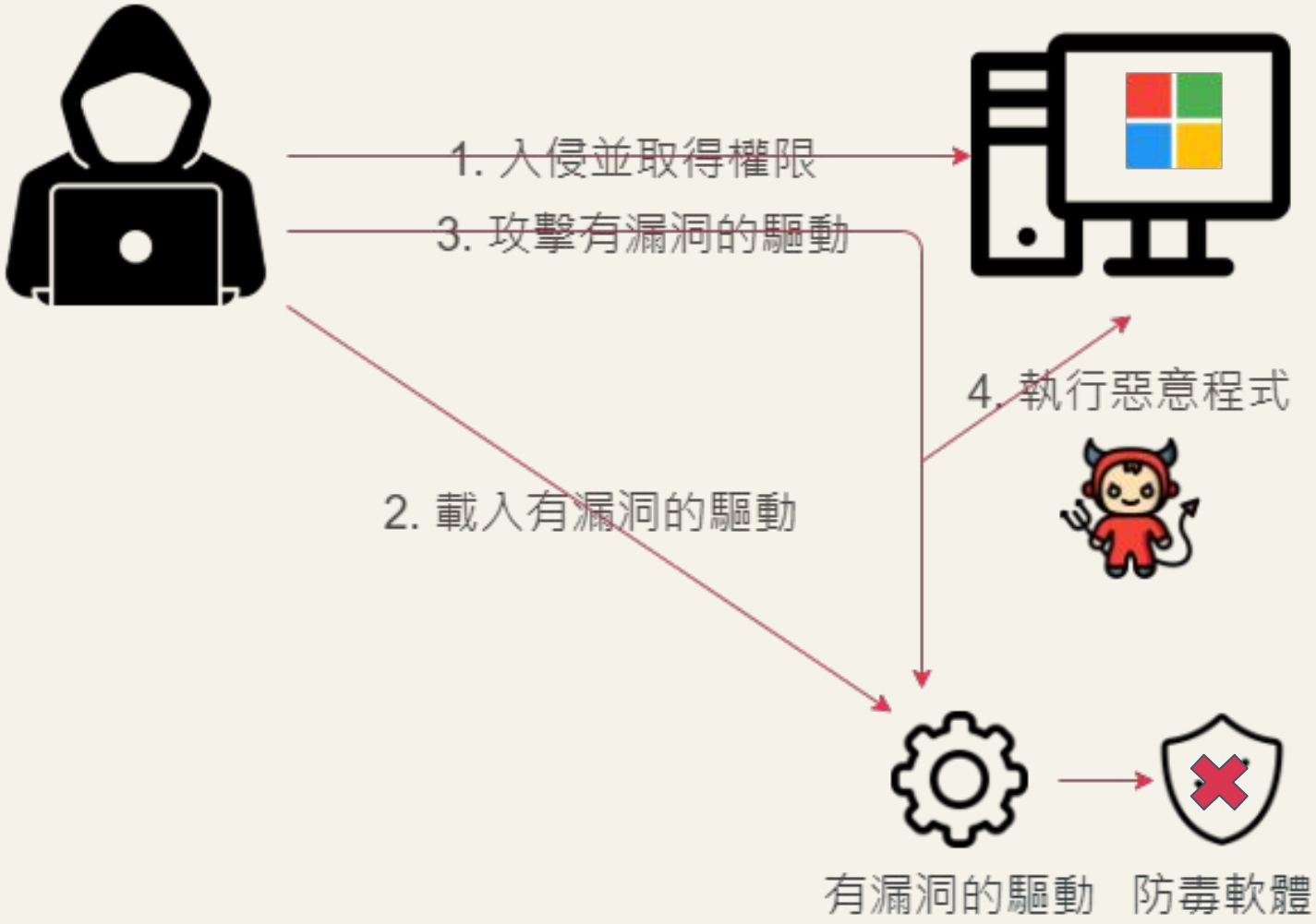
攻擊防毒軟體－BYOVD

TEAMT5 杜浦數位安全



攻擊防毒軟體－BYOVD

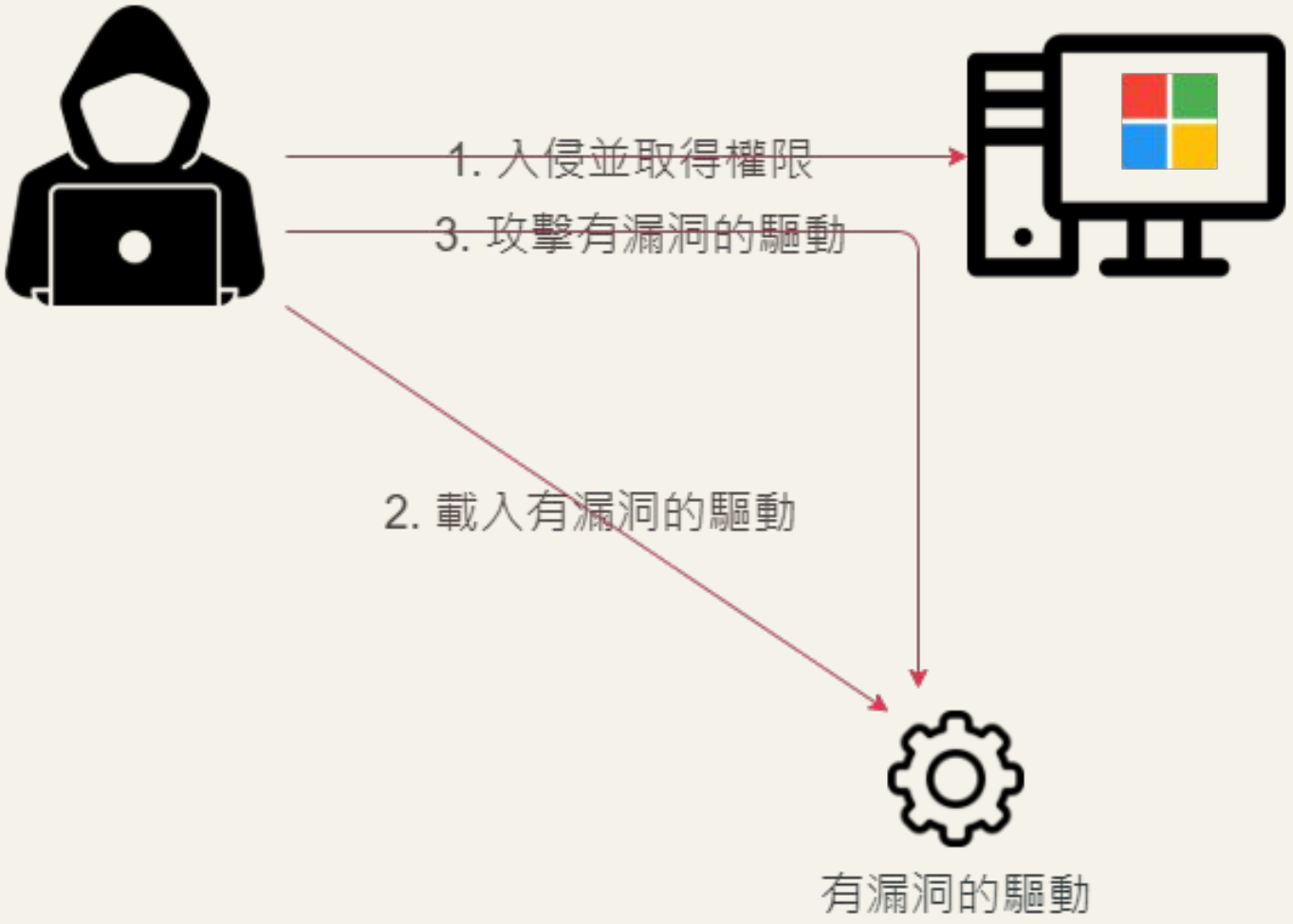
TEAMT5 杜浦數位安全



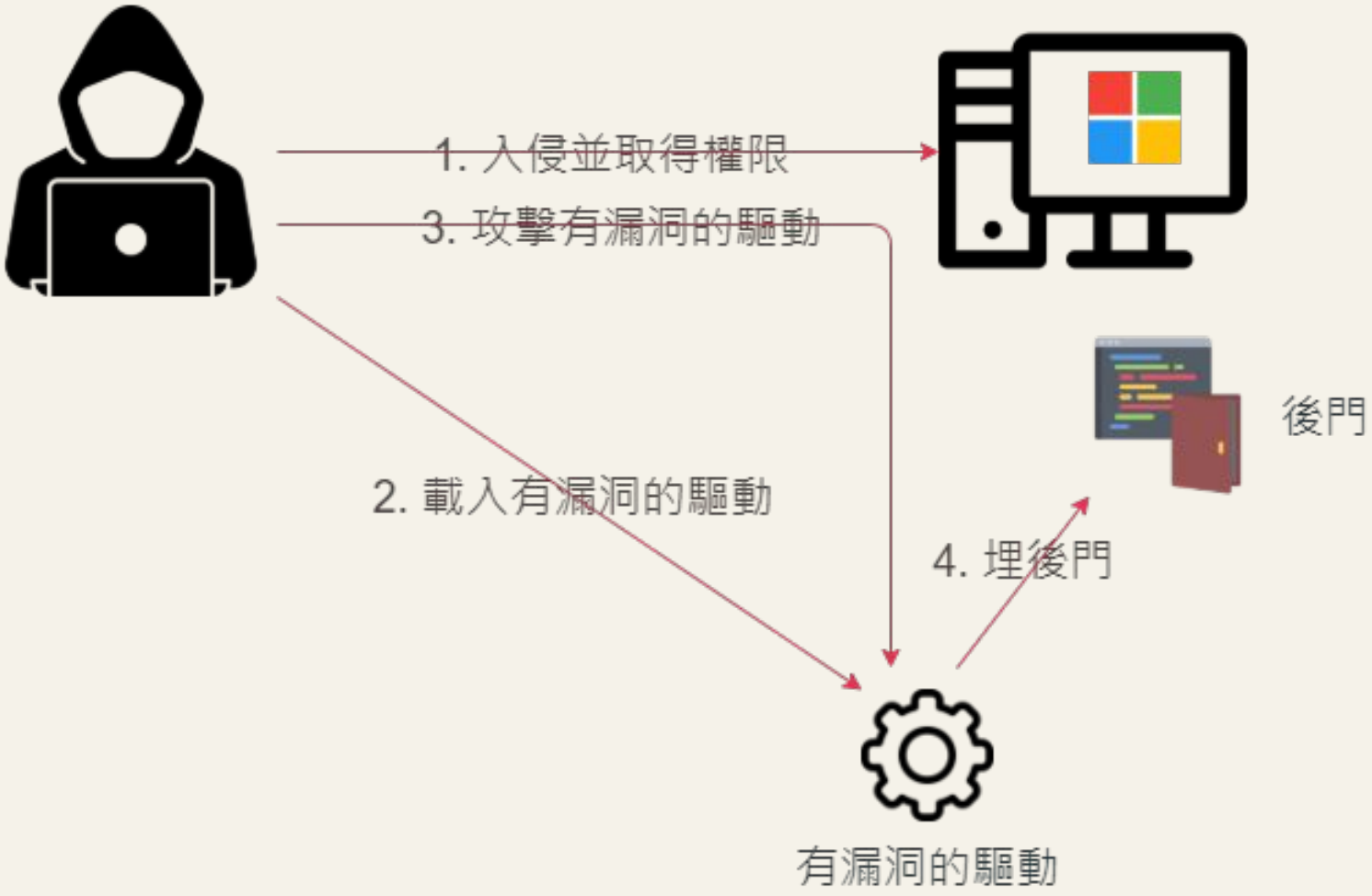
BYOVD 的目的

- 攻擊防毒軟體
- **埋後門**
- 隱藏蹤跡
- 破壞系統

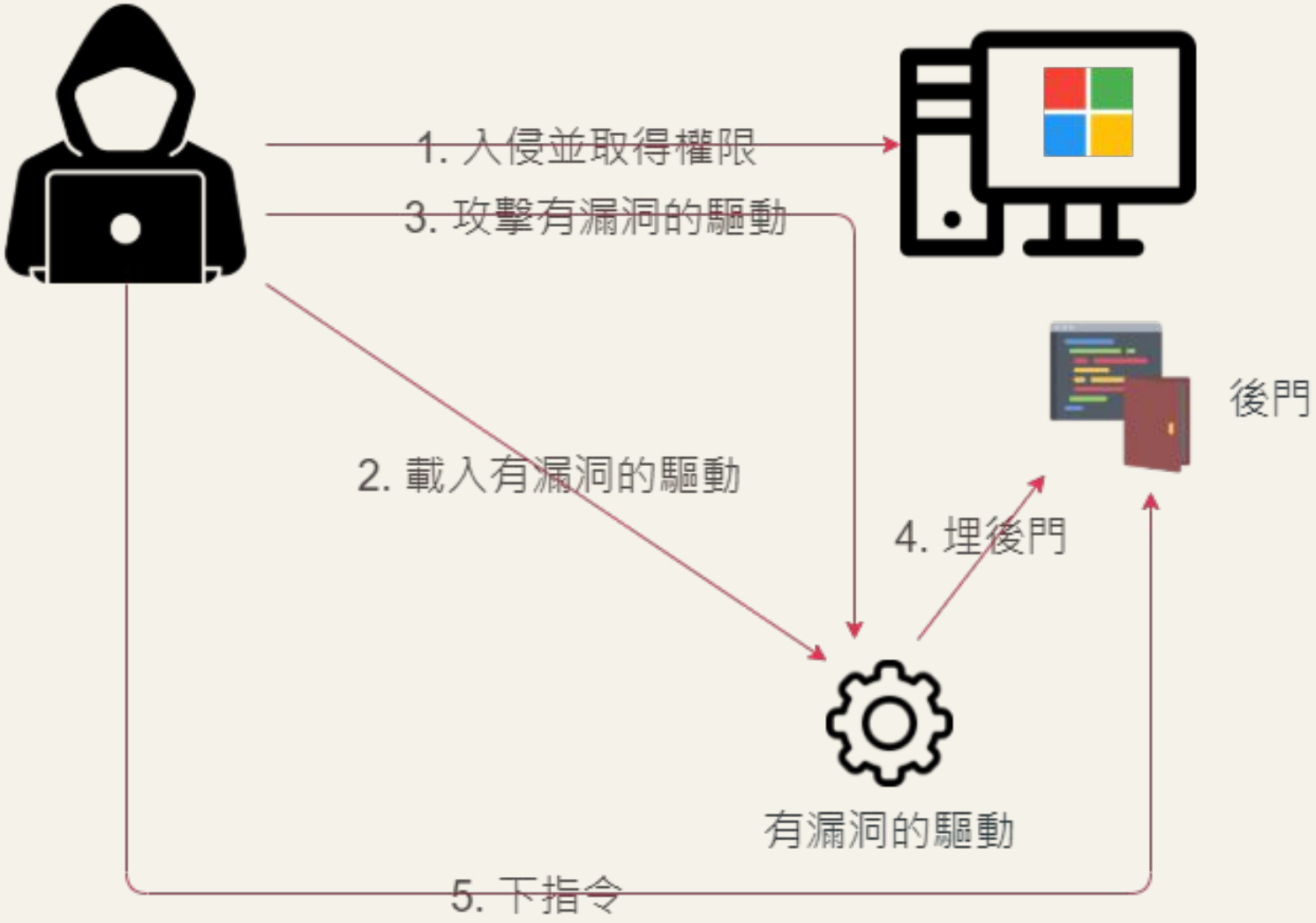
埋後門



埋後門



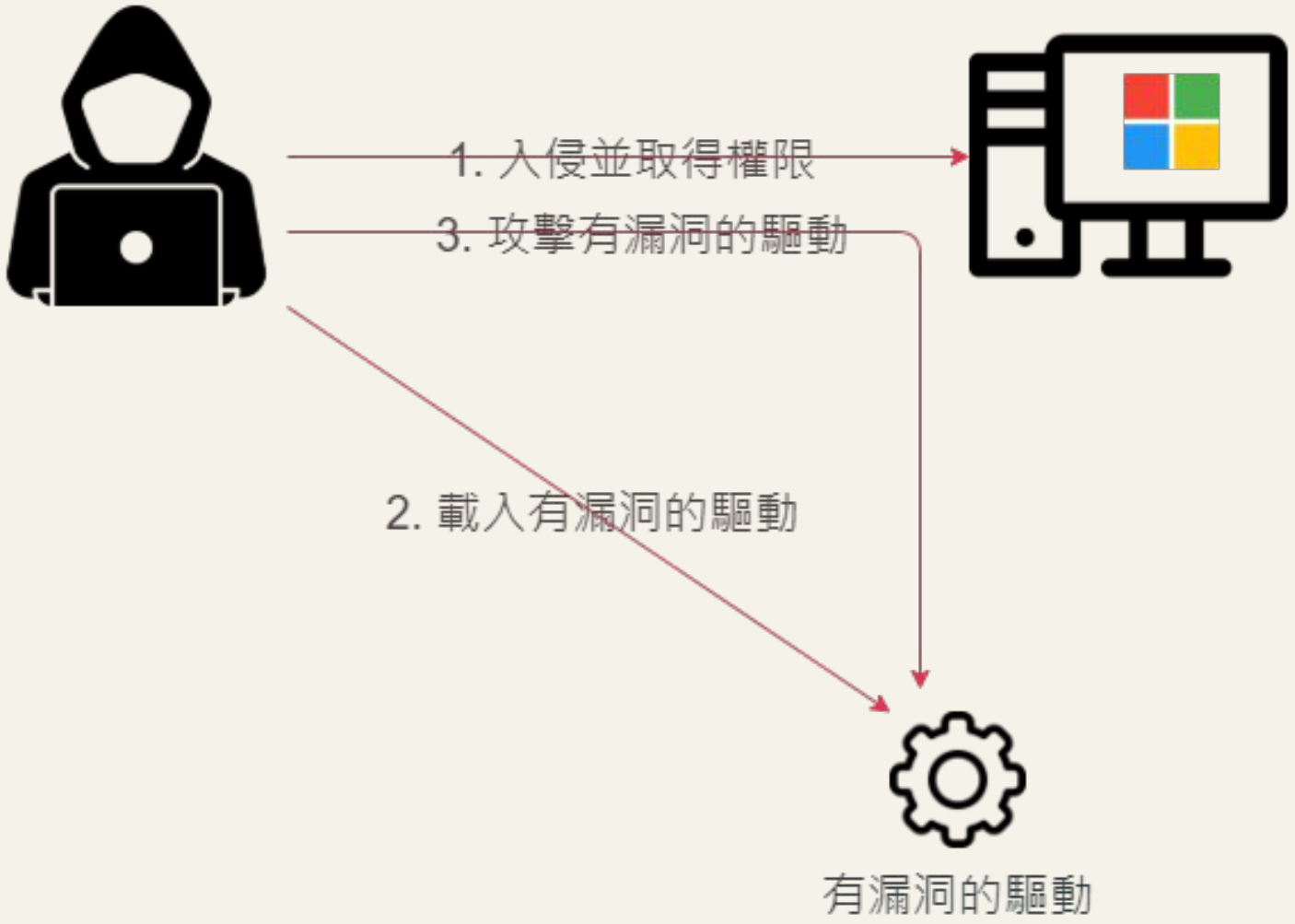
埋後門



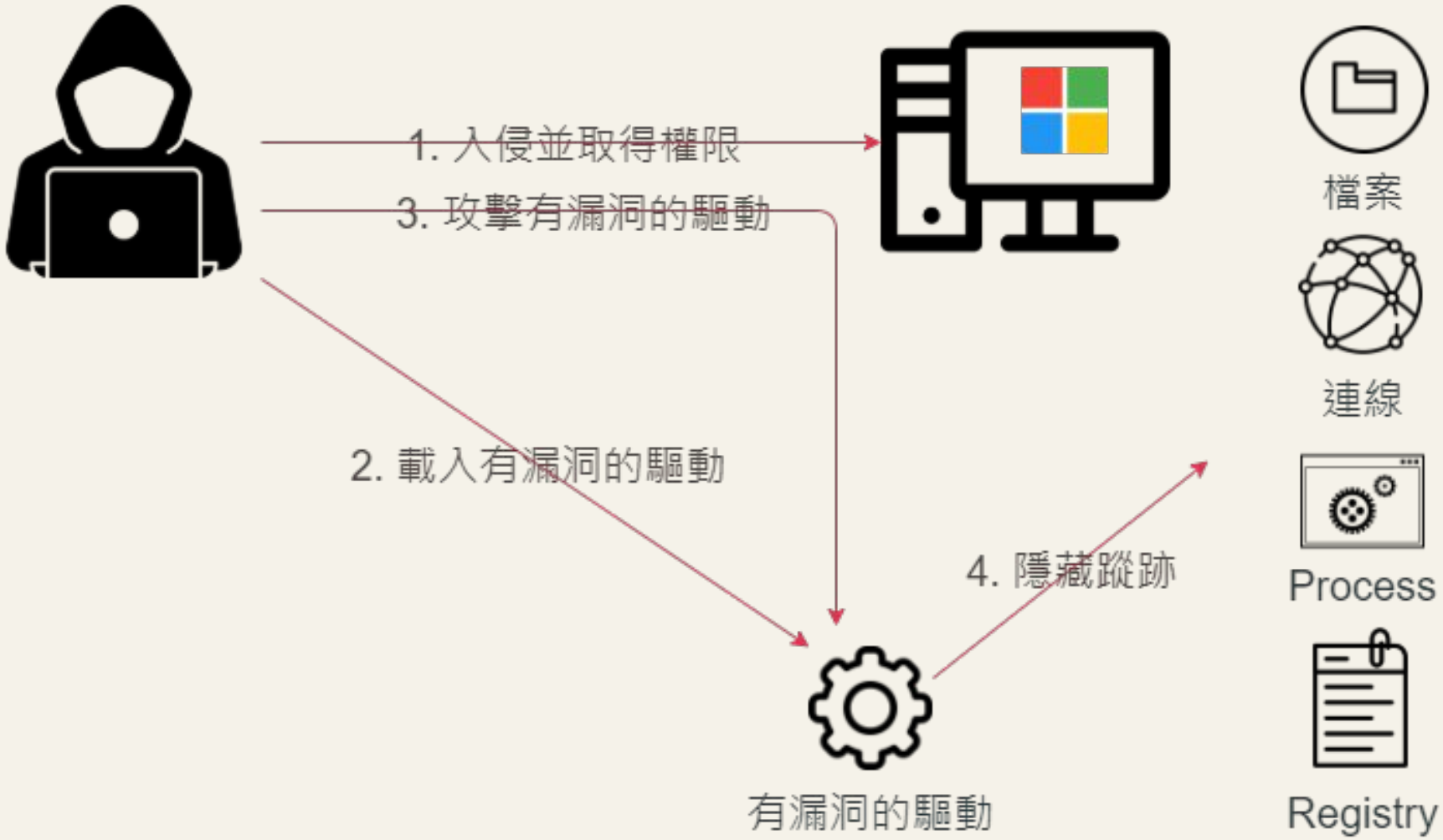
BYOVD 的目的

- 攻擊防毒軟體
- 埋後門
- **隱藏蹤跡**
- 破壞系統

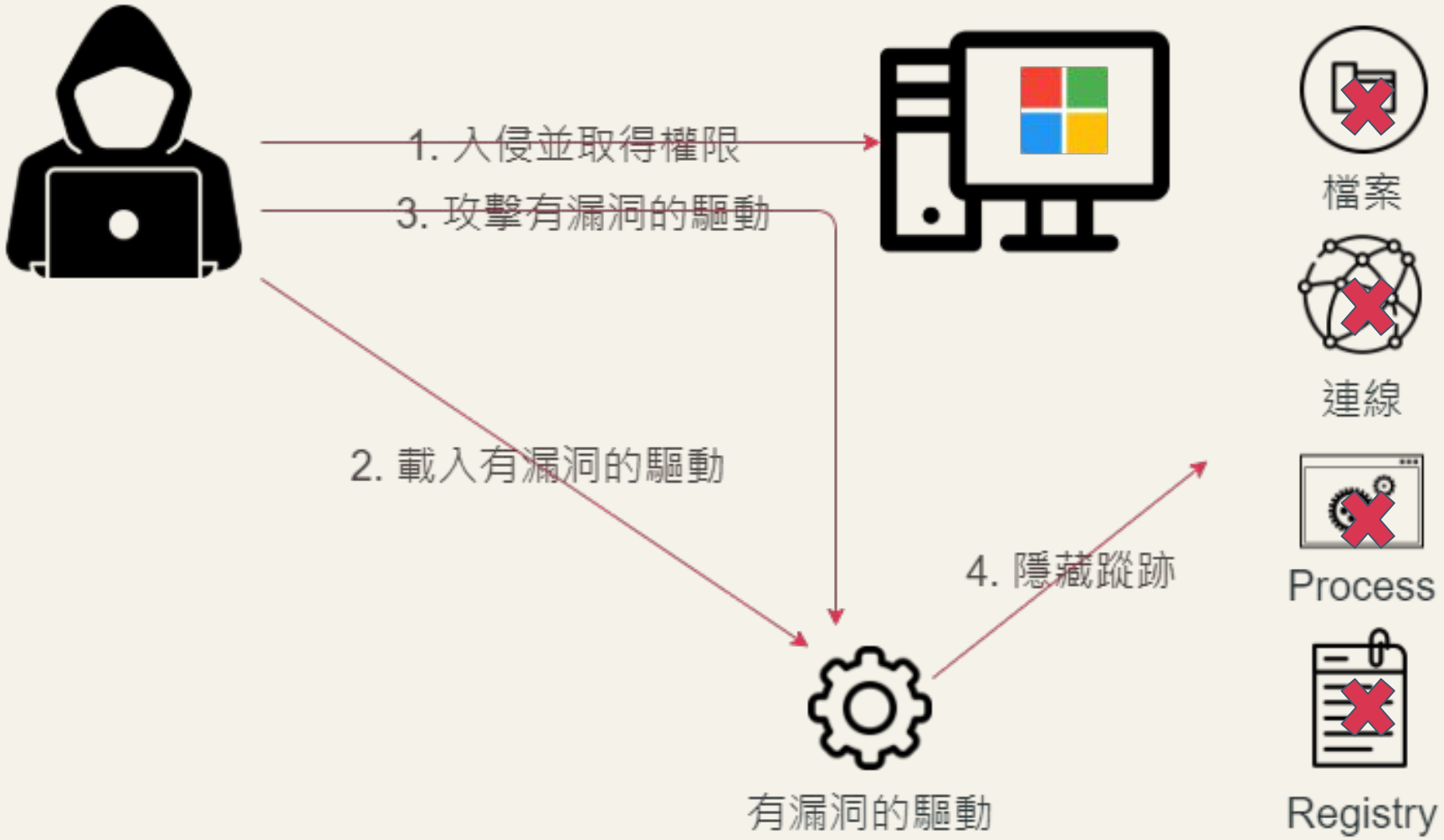
隱藏蹤跡



隱藏蹤跡


1. 入侵並取得權限
3. 攻擊有漏洞的驅動
2. 載入有漏洞的驅動
4. 隱藏蹤跡
檔案
連線
Process
Registry
有漏洞的驅動

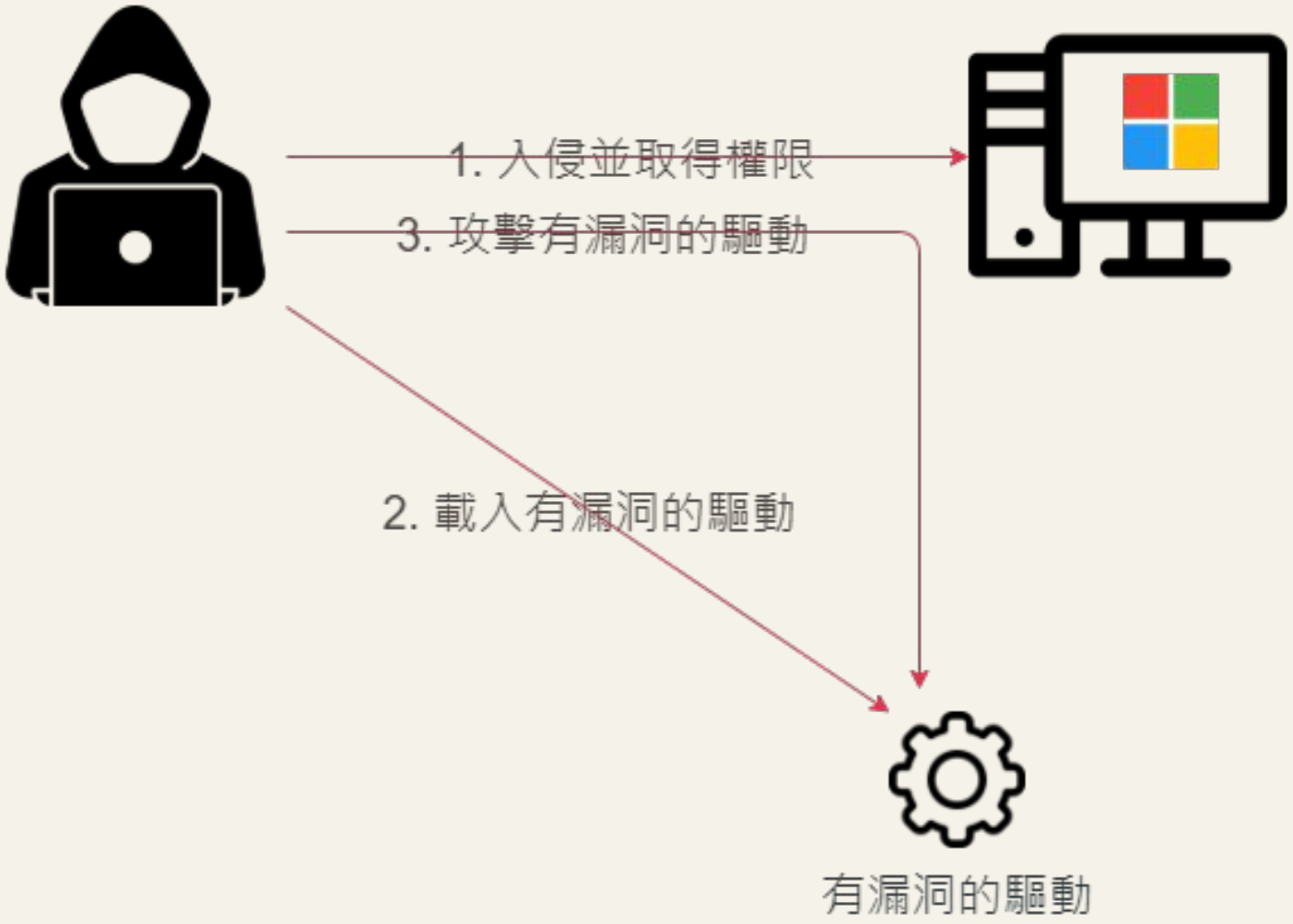
隱藏蹤跡


1. 入侵並取得權限
3. 攻擊有漏洞的驅動
2. 載入有漏洞的驅動
4. 隱藏蹤跡
檔案
連線
Process
Registry
有漏洞的驅動

BYOVD 的目的

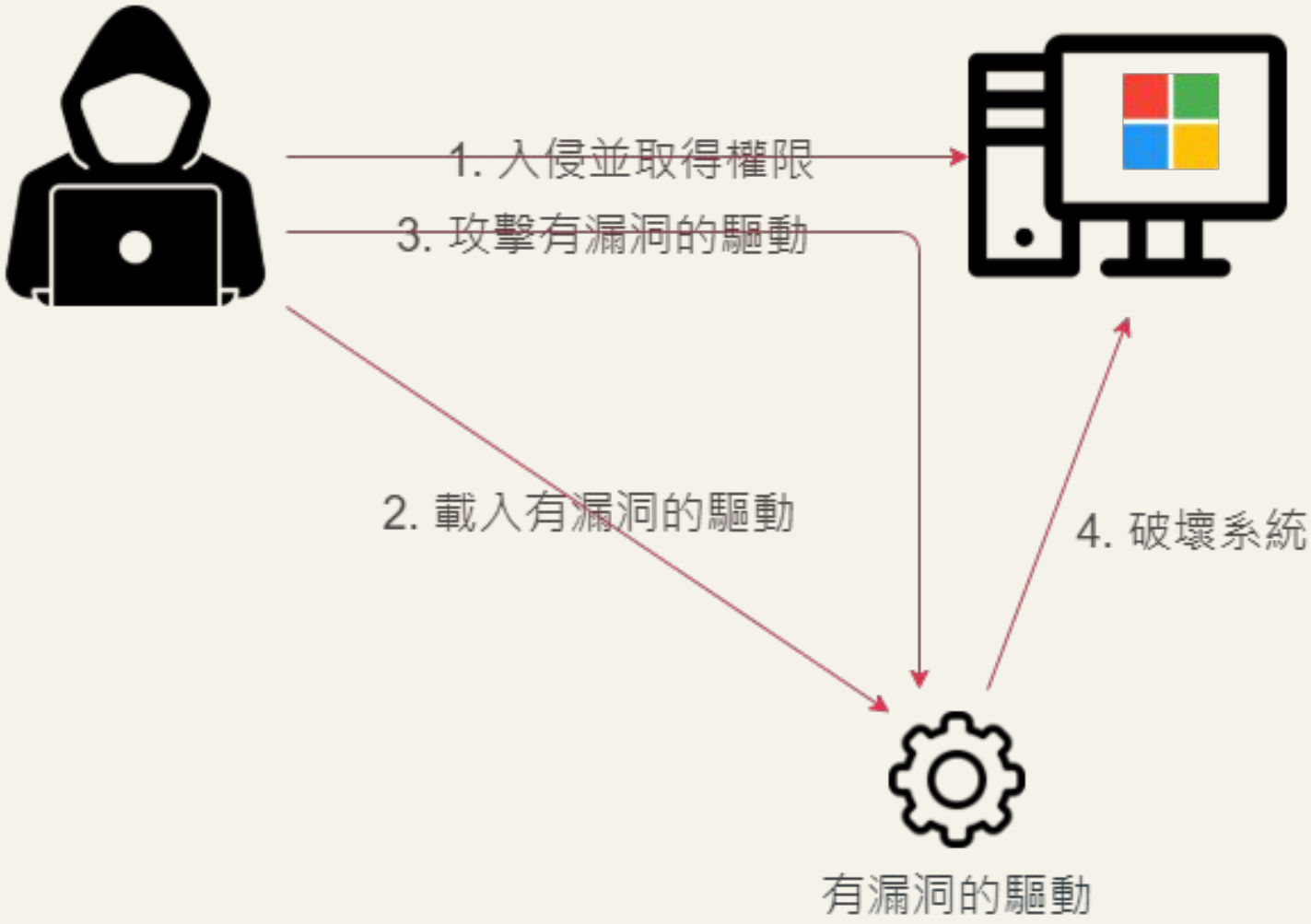
- 攻擊防毒軟體
- 埋後門
- 隱藏蹤跡
- **破壞系統**

破壞系統



破壞系統

TEAMT5
杜 浦 數 位 安 全



案例分析

實際案例

- 2022 BlackByte, RTCore64.sys, 攻擊防毒軟體
- 2021 Iron Tiger, cpuz141.sys, 埋後門
- 2021 GhostEmperor, dbk64.sys, 隱藏蹤跡
- 2022 Hermetic, epmntdrv.sys, 破壞系統

實際案例

- **2022 BlackByte, RTCore64.sys, 攻擊防毒軟體**
- 2021 Iron Tiger, cpuz141.sys, 埋後門
- 2021 GhostEmperor, dbk64.sys, 隱藏蹤跡
- 2022 Hermetic, epmntdrv.sys, 破壞系統

BlackByte

- 攻擊公開於 2022/10
- 濫用微星科技(Micro-Star International)的 RTCore64.sys 驅動的任意讀寫漏洞(CVE-2019-16098)攻擊防毒軟體
- 執行勒索軟體

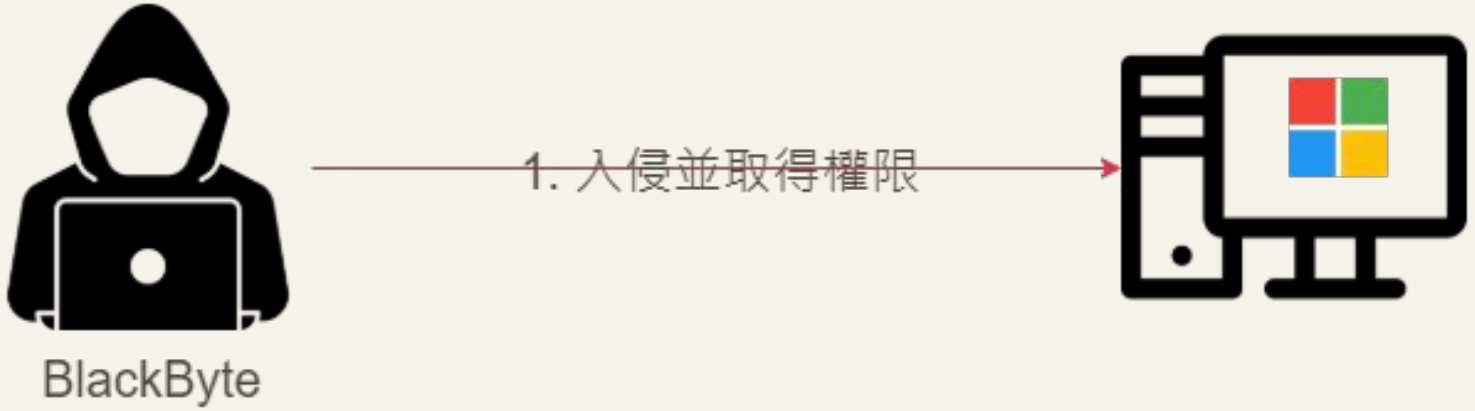
RTCore64.sys一漏洞成因

TEAMT5 杜浦數位安全

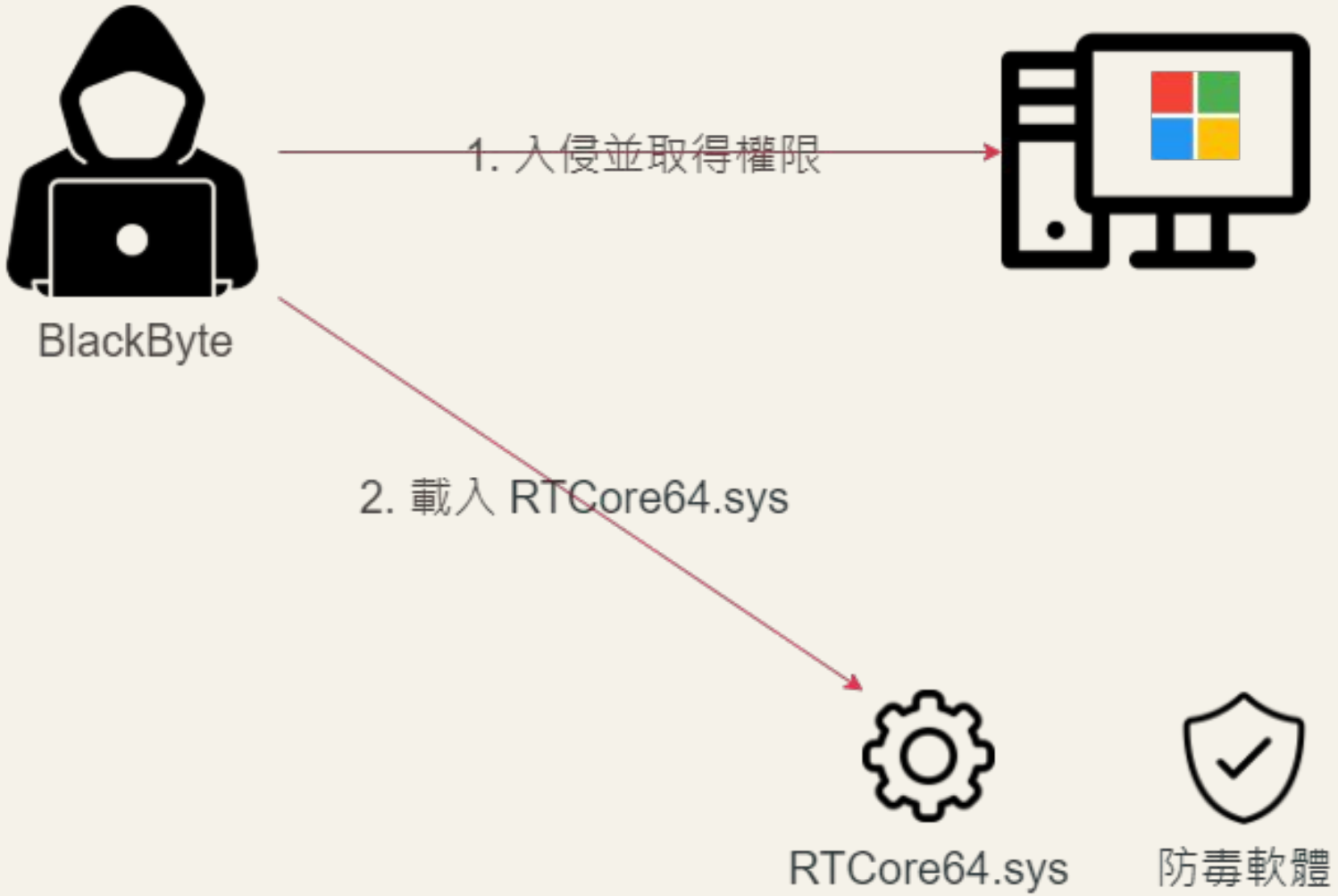
```
case 0x8000204C:
  if ( (_DWORD)InputLength == 48 )
  {
    *(_QWORD *)&UserInput_8 = *((_QWORD *)pUserInput + 1);
    if ( *(_QWORD *)&UserInput_8 )
    {
      switch ( *((_DWORD *)pUserInput + 6) )
      {
        case 1:
          *(_BYTE *)(*((unsigned int *)pUserInput + 5) + *(_QWORD *)&UserInput_8) = pUserInput[28];
          break;
        case 2:
          *(_WORD *)(*((unsigned int *)pUserInput + 5) + *(_QWORD *)&UserInput_8) = *((_WORD *)pUserInput + 14);
          break;
        case 4:
          *(_DWORD *)(*((unsigned int *)pUserInput + 5) + *(_QWORD *)&UserInput_8) = *((_DWORD *)pUserInput + 7);
          break;
      }
      pIrp_a2->IoStatus.Status = 0;
      pIrp_a2->IoStatus.Information = 48i64;
    }
    else
    {
      pIrp_a2->IoStatus.Status = -1073741670;
    }
  }
  else
  {
    pIrp_a2->IoStatus.Status = -1073741811;
  }
  break;
```

攻擊者可以任意寫入目標位址

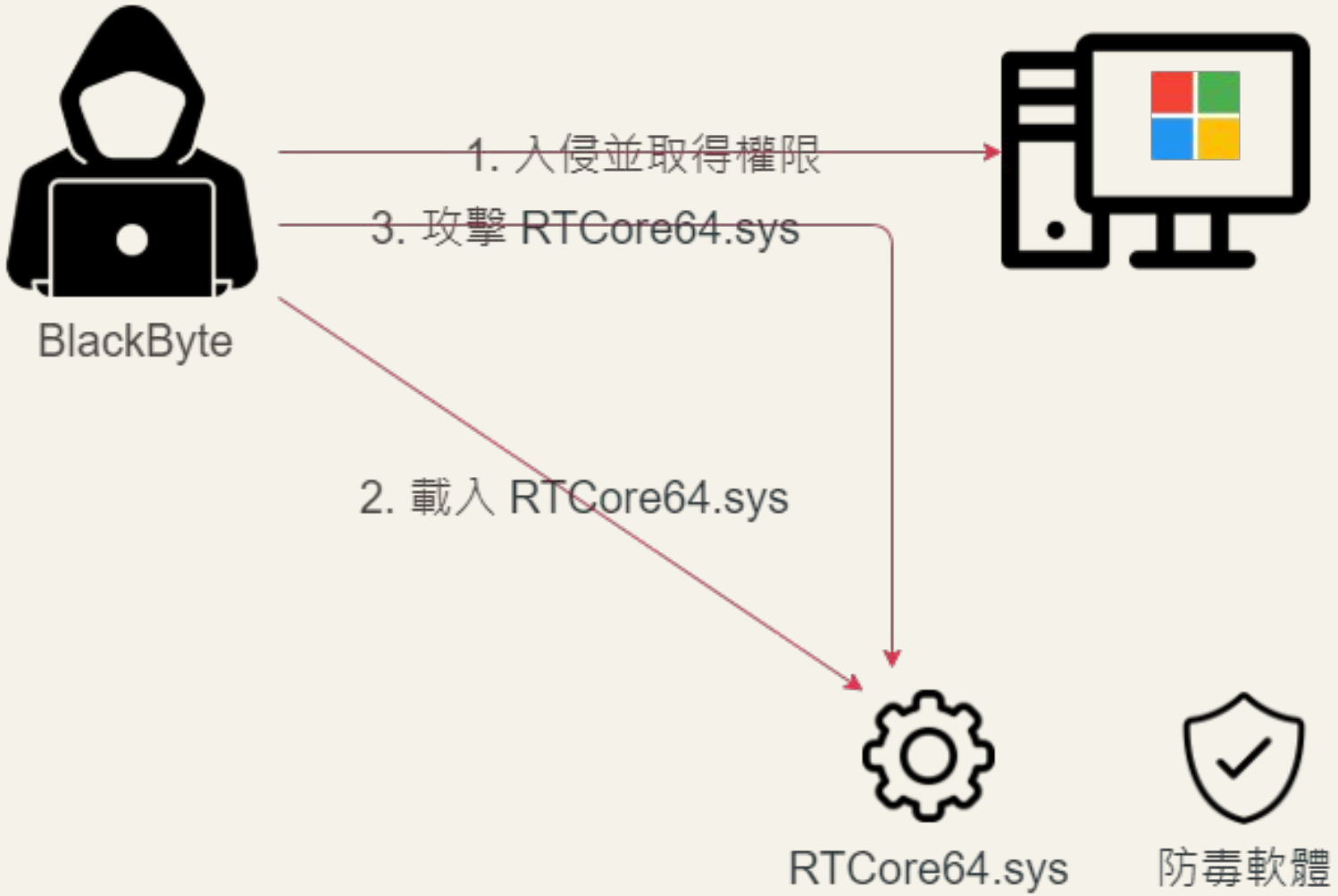
BlackByte－攻擊防毒軟體



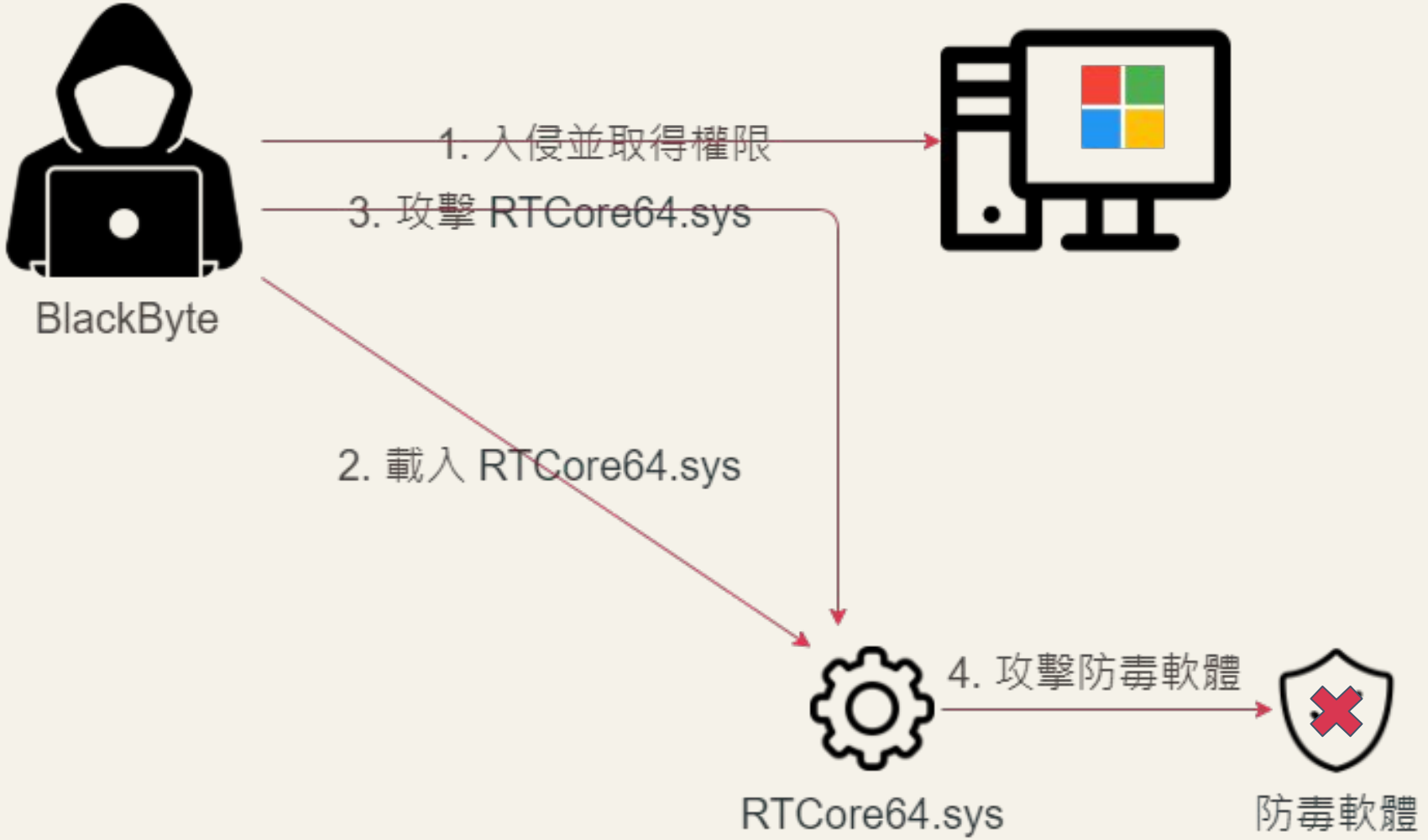
BlackByte－攻擊防毒軟體



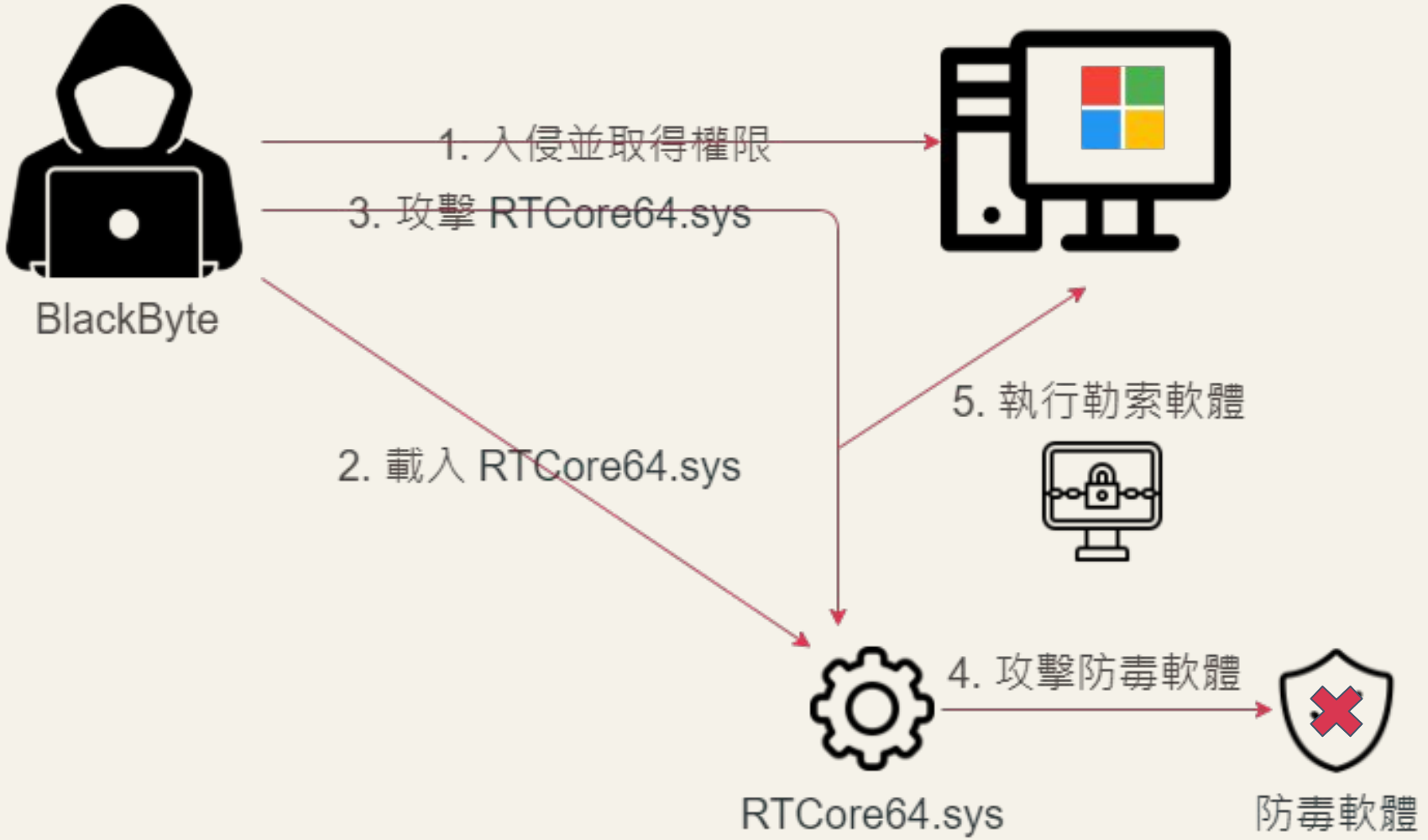
BlackByte－攻擊防毒軟體



BlackByte－攻擊防毒軟體



BlackByte－攻擊防毒軟體



實際案例

- 2022 BlackByte, RTCore64.sys, 攻擊防毒軟體
- **2021 Iron Tiger, cpuz141.sys, 埋後門**
- 2021 GhostEmperor, dbk64.sys, 隱藏蹤跡
- 2022 Hermetic, epmntdrv.sys, 破壞系統

Iron Tiger

- 攻擊公開於 2021/04
- 又稱作 APT27、LuckyMouse
- 濫用 CPUID 的 cpuz141.sys 驅動的任意物理記憶體讀寫漏洞 (CVE-2017-15303) 埋後門
- 與 C2 連線接收指令

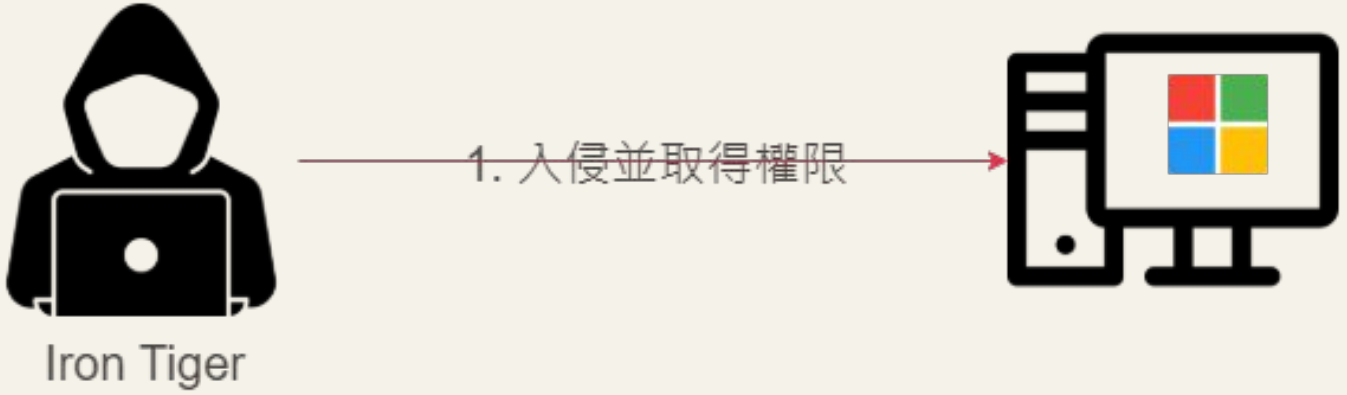
cpuz141.sys一漏洞成因

TEAMT5 杜浦數位安全

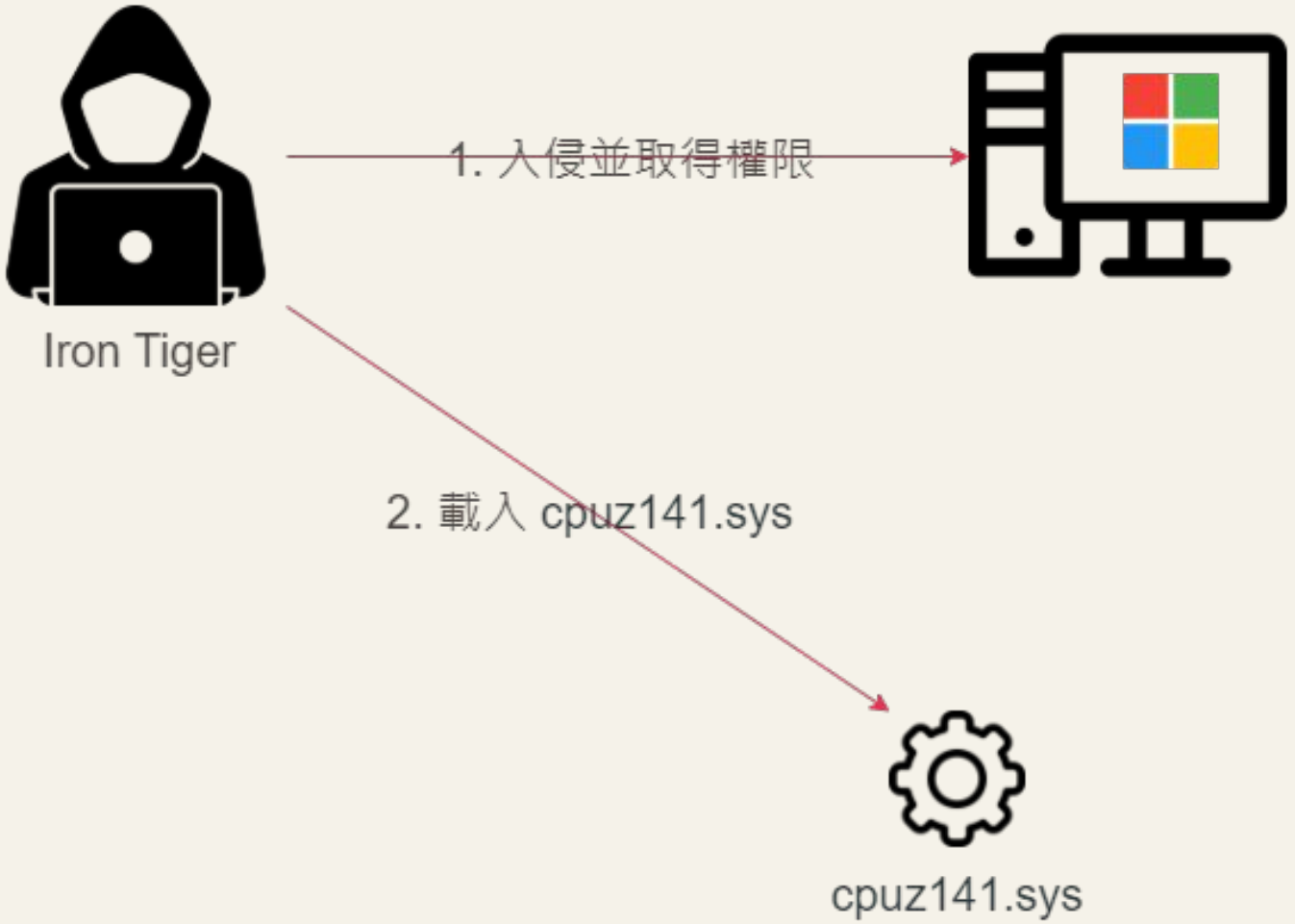
```
case 0x9C402430:
  if ( IoStackLocation_v3->Parameters.Read.Length < 8 || IoStackLocation_v3->Parameters.Create.Options < 0xC )
  {
    pIrp_a2->IoStatus.Information = 0i64;
    pIrp_a2->IoStatus.Status = -1073741789;
  }
  else
  {
    UserInput.HighPart = *(_DWORD *)pUserInput;
    UserInput.LowPart = *((_DWORD *)pUserInput + 1);
    UserInput_8 = *((_DWORD *)pUserInput + 2);
    v19 = (_QWORD *)sub_11170(UserInput.QuadPart, 4u);
    if ( v19 )
    {
      *(_DWORD *)(UserInput.QuadPart - *v19 + v19[1]) = UserInput_8;
      *(_DWORD *)pUserInput = 286331153;
    }
    else
    {
      PhysicalMemory = MmMapIoSpace(UserInput, 4ui64, MmNonCached);
      *PhysicalMemory = UserInput_8;
      MmUnmapIoSpace(PhysicalMemory, 4ui64);
      *(_DWORD *)pUserInput = 0x22222222;
    }
    *((_DWORD *)pUserInput + 1) = UserInput_8;
    pIrp_a2->IoStatus.Information = 8i64;
    pIrp_a2->IoStatus.Status = 0;
  }
  break;
```

攻擊者任意映射並寫入目標物理記憶體

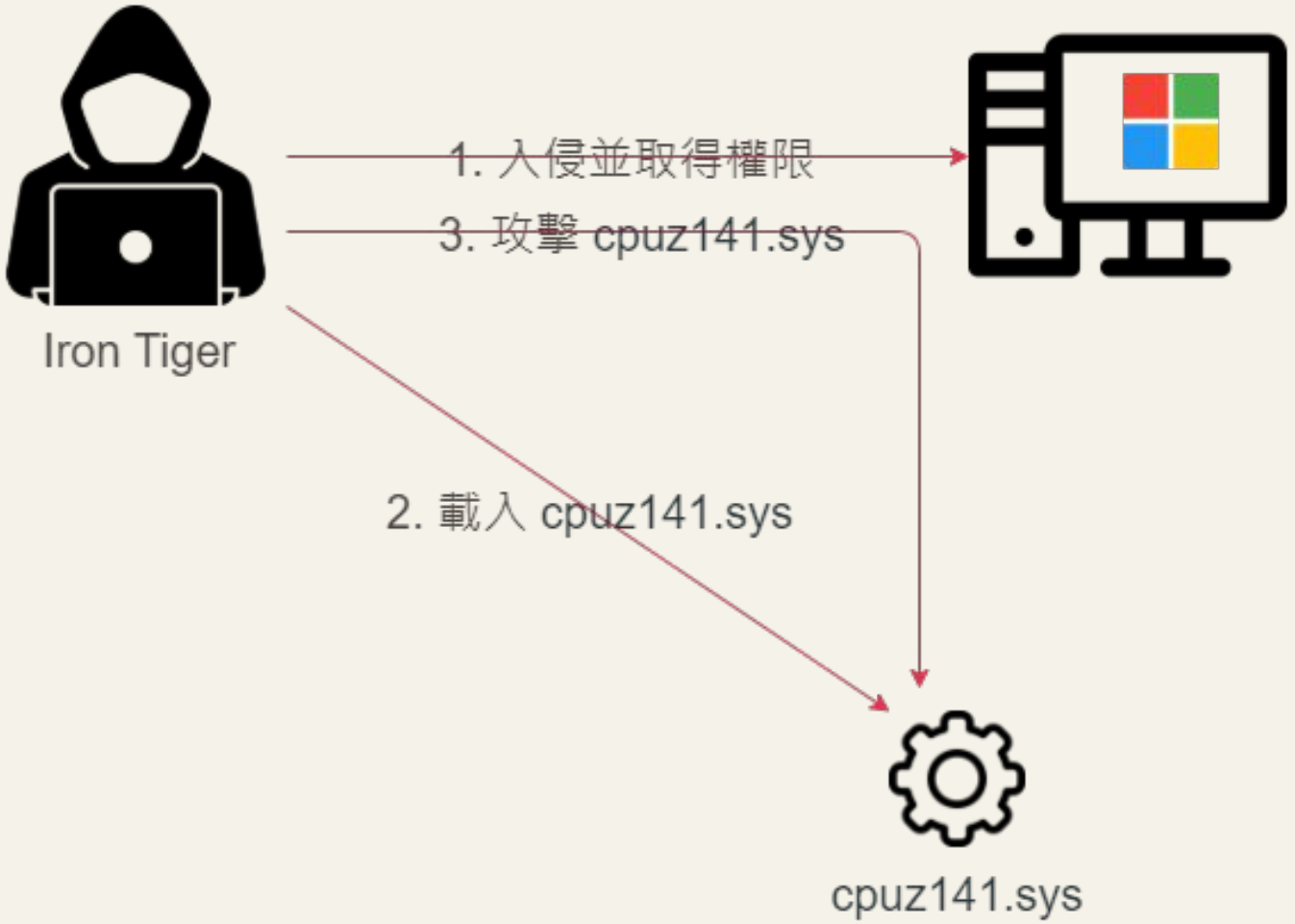
Iron Tiger一埋後門



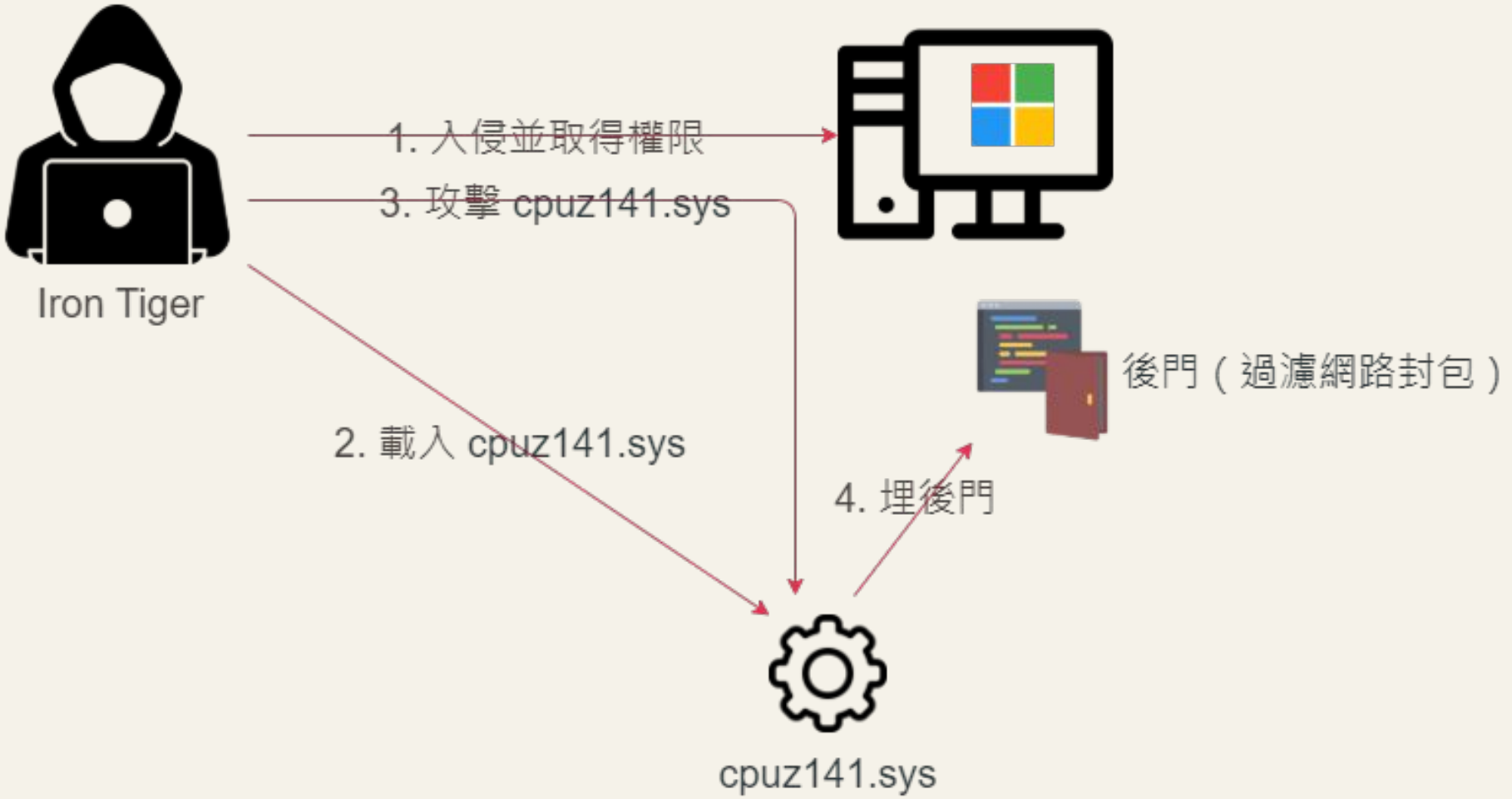
Iron Tiger一埋後門



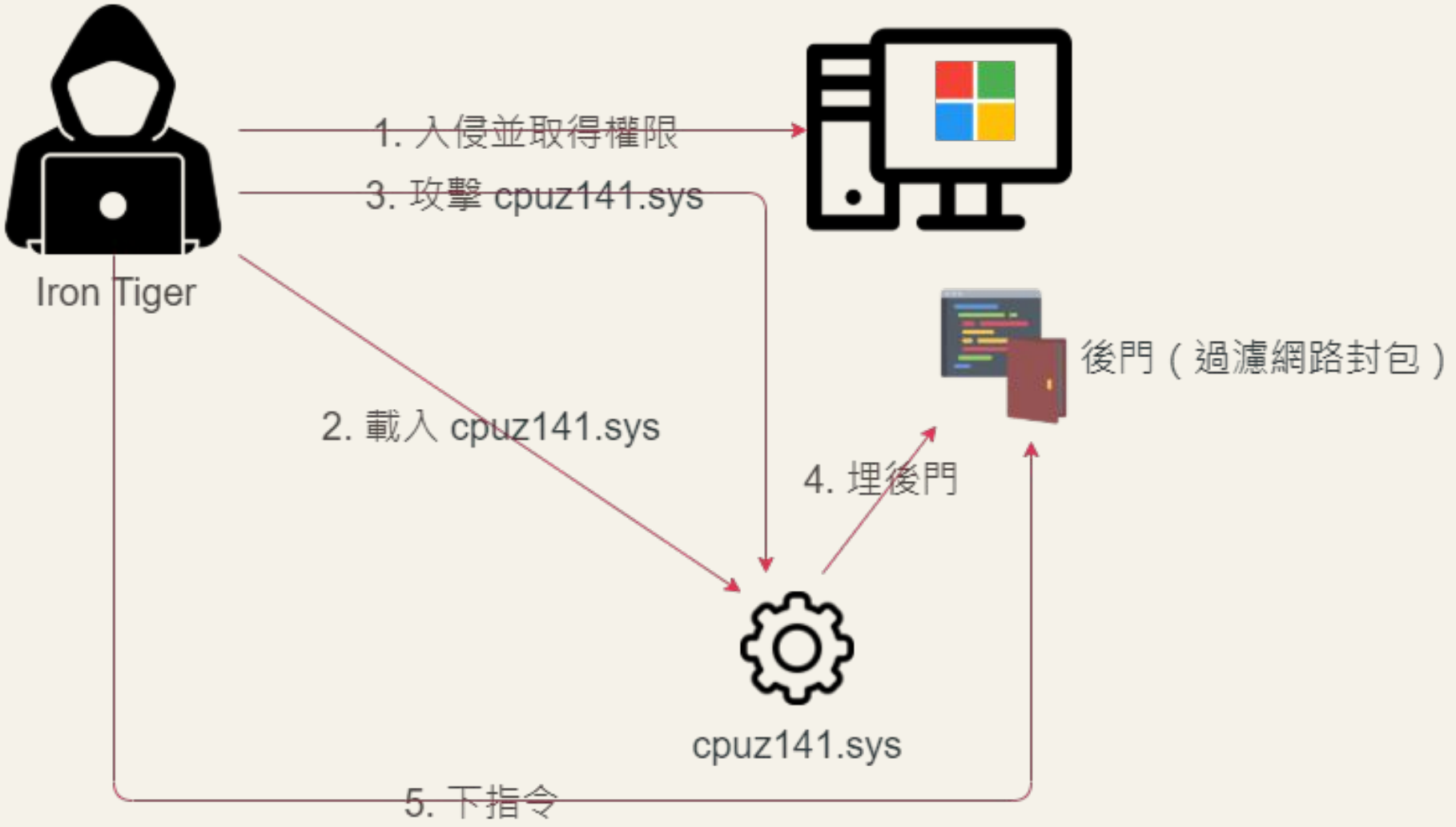
Iron Tiger一埋後門



Iron Tiger一埋後門



Iron Tiger一埋後門



實際案例

- 2022 BlackByte, RTCore64.sys, 攻擊防毒軟體
- 2021 Iron Tiger, cpuz141.sys, 埋後門
- **2021 GhostEmperor, dbk64.sys, 隱藏蹤跡**
- 2022 Hermetic, epmntdrv.sys, 破壞系統

GhostEmperor

- 攻擊公開於 2021/09
- 主要攻擊馬來西亞、泰國、越南、印尼等地區
- 濫用 CheatEngine 的 dbk64.sys 驅動的記憶體讀寫**功能**隱藏蹤跡
- 隱藏惡意程式相關的檔案、Process、Registry、連線

dbk64.sys－功能濫用

TEAMT5 杜浦數位安全

1. 用 IOCTL_CE_ALLOCATEMEM_NONPAGED 申請一塊記憶體
2. 用 IOCTL_CE_MAP_MEMORY 把這塊記憶體映射到 user mode process
3. 在 user space process 寫入 shellcode 到那塊記憶體
4. 用 IOCTL_CE_UNMAP_MEMORY 取消映射
5. 用 IOCTL_CE_EXECUTE_CODE 執行 shellcode

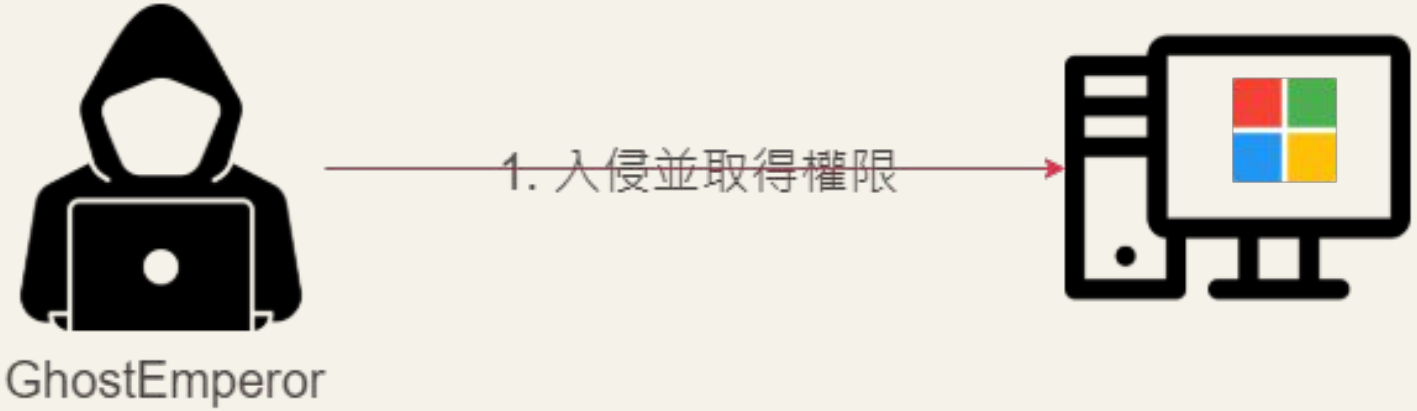
dbk64.sys－功能濫用

TEAMT5 杜浦數位安全

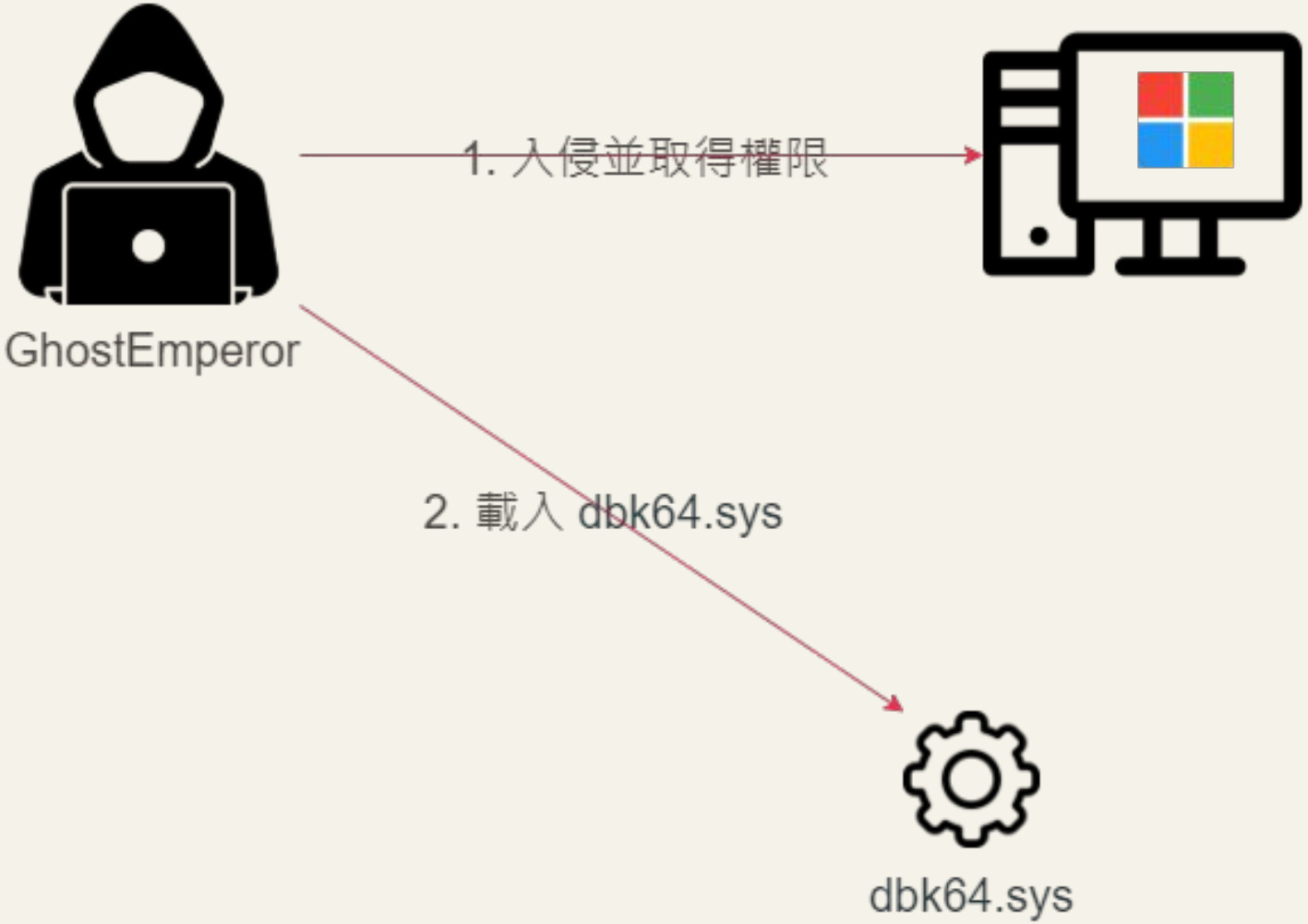
```
case IOCTL_CE_EXECUTE_CODE:
	{
		typedef NTSTATUS (*PARAMETERLESSFUNCTION)(UINT64 parameters);
		PARAMETERLESSFUNCTION functiontocall;

		struct input
		{
			UINT64  functionaddress; //function address to call
			UINT64  parameters;
		} *inp=Irp->AssociatedIrp.SystemBuffer;
		DbgPrint("IOCTL_CE_EXECUTE_CODE\n");

		functiontocall=(PARAMETERLESSFUNCTION)(UINT_PTR)(inp->functionaddress);

		__try
		{
			ntStatus=functiontocall(inp->parameters);
			DbgPrint("Still alive\n");
			ntStatus=STATUS_SUCCESS;
		}
		__except(1)
		{
			DbgPrint("Exception occured\n");
			ntStatus=STATUS_UNSUCCESSFUL;
		}

		break;
	}
```

攻擊者可以任意執行 shellcode

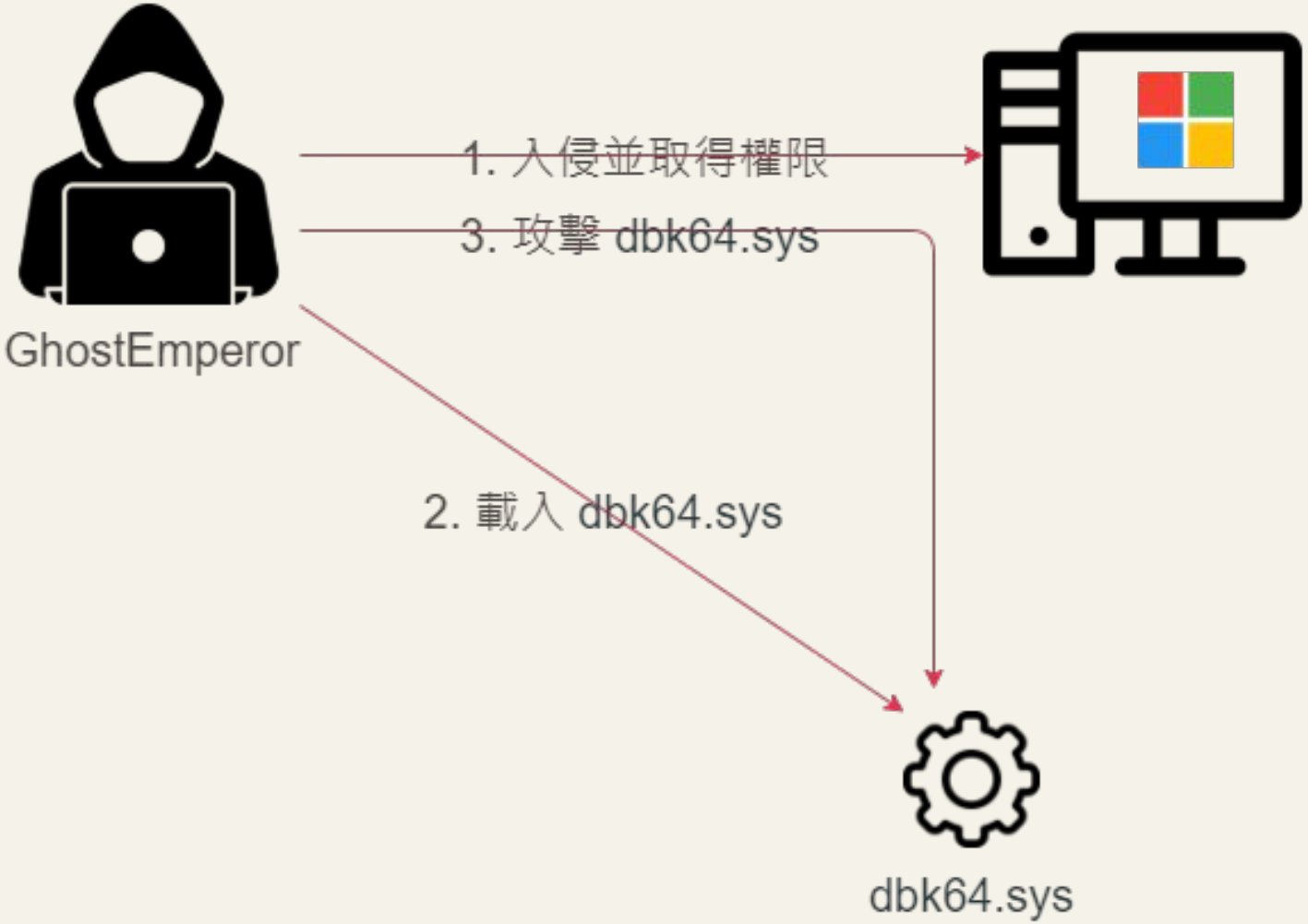
GhostEmperor－隱藏蹤跡



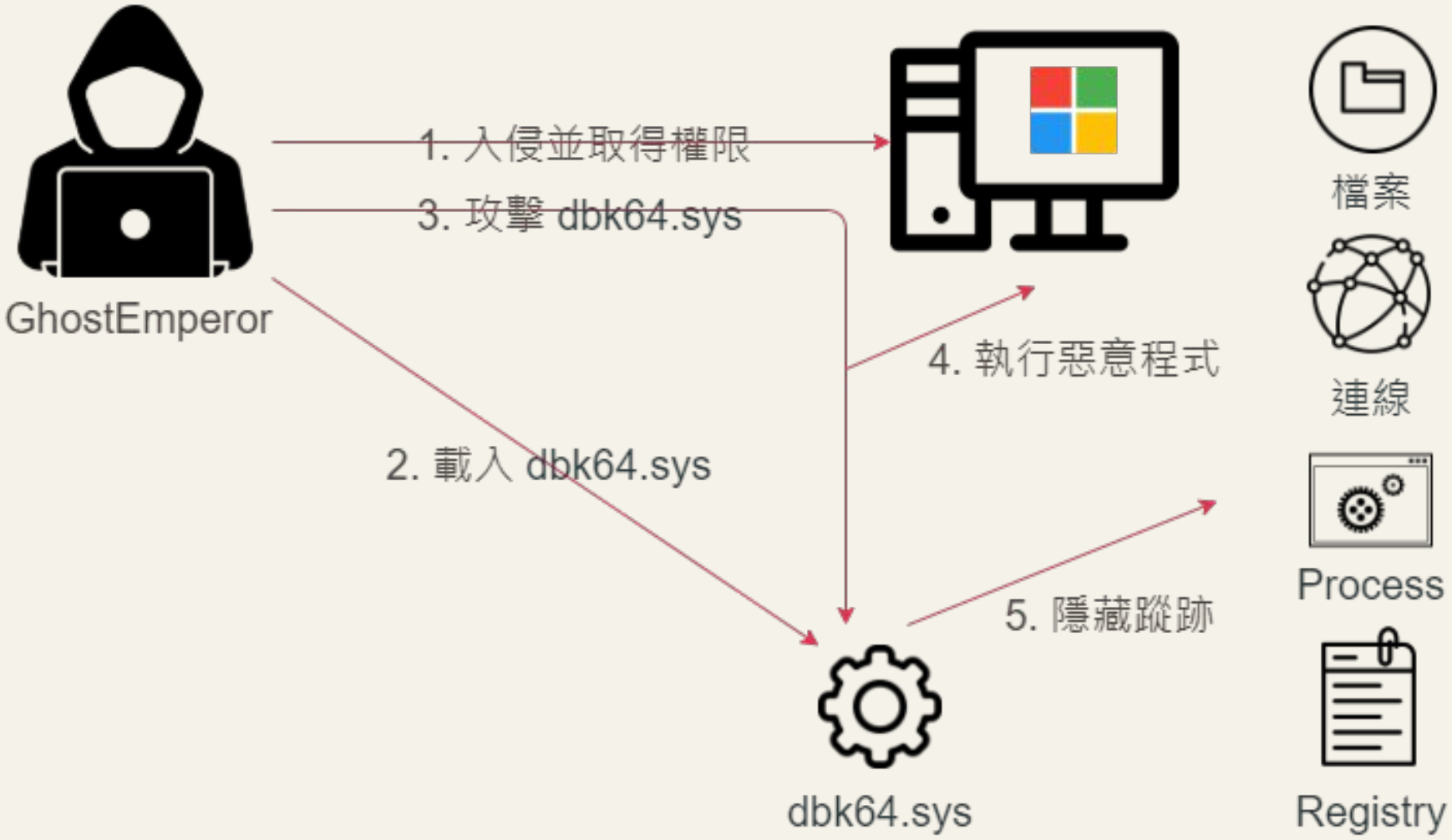
GhostEmperor－隱藏蹤跡



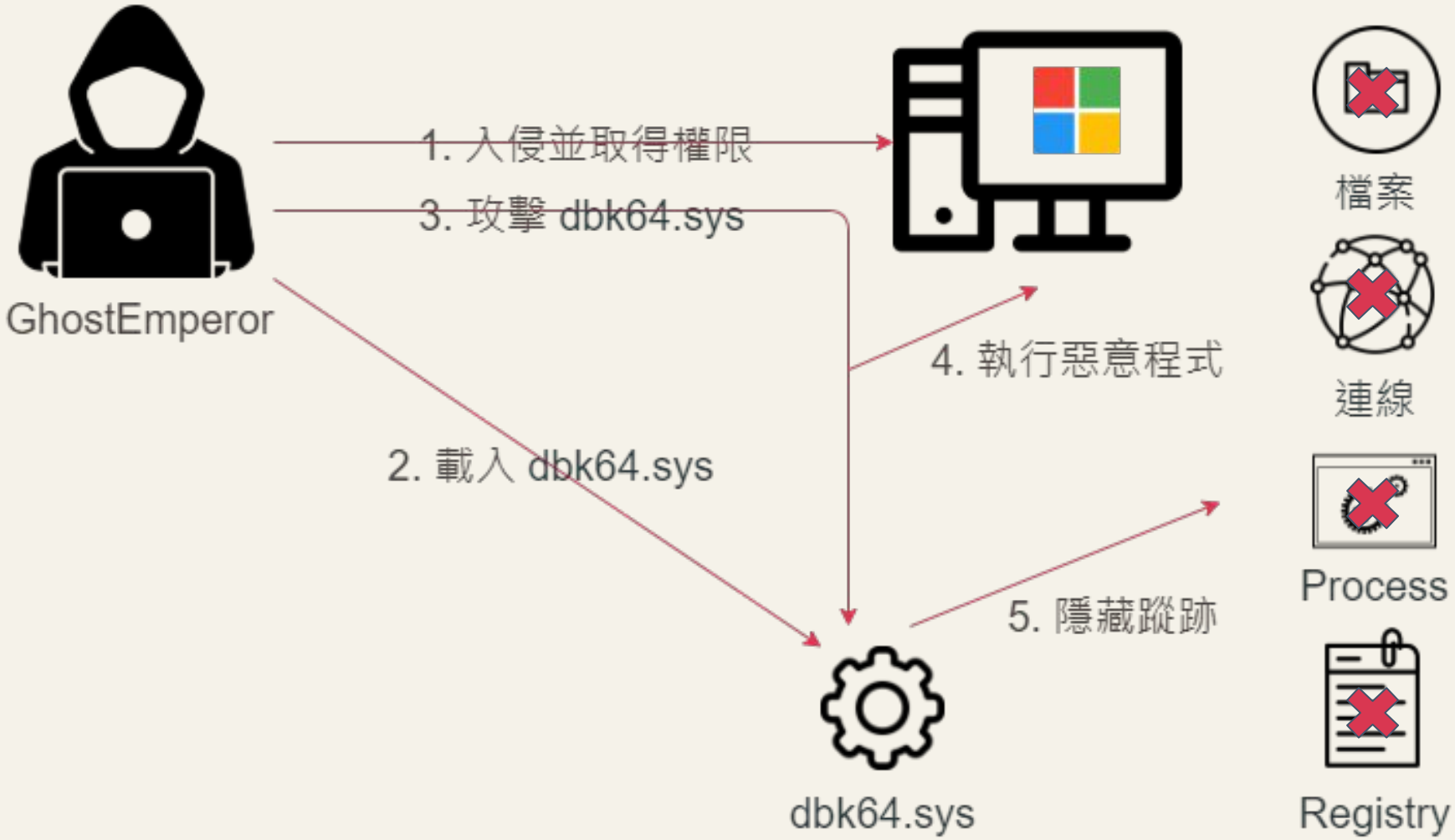
GhostEmperor－隱藏蹤跡



GhostEmperor－隱藏蹤跡



GhostEmperor－隱藏蹤跡



實際案例

- 2022 BlackByte, RTCore64.sys, 攻擊防毒軟體
- 2021 Iron Tiger, cpuz141.sys, 埋後門
- 2021 GhostEmperor, dbk64.sys, 隱藏蹤跡
- **2022 Hermetic, epmntdrv.sys, 破壞系統**

Hermetic

- 攻擊公開於 2022/03
- 在 2022/02/24 俄羅斯軍隊入侵烏克蘭的前一天針對烏克蘭的 wiper
- 濫用 Hermetica Digital Ltd. 的 epmntdrv.sys 驅動的磁碟讀寫**功能**
- 破壞系統且無法復原

epmntdrv.sys一功能濫用

TEAMT5 杜浦數位安全

```
RtlInitUnicodeString(&DestinationString, L"Disk");
CurrentDeviceObject = v7;
do
{
  v9 = CurrentDeviceObject->DriverObject;
  if ( v9 )
  {
    if ( !RtlCompareUnicodeString(&v9->DriverExtension->ServiceKeyName, &DestinationString, 1u) )
      goto LABEL_21;
    if ( v7 != CurrentDeviceObject )
      ObfDereferenceObject(CurrentDeviceObject);
  }
  CurrentDeviceObject = IoGetLowerDeviceObject(CurrentDeviceObject);
}
while ( CurrentDeviceObject );
CurrentDeviceObject = 0i64;
LABEL_21:
if ( CurrentDeviceObject )
{
  ObfDereferenceObject(v7);
  FileObject_v5->FsContext2 = CurrentDeviceObject;
  pIrp_a2->IoStatus.Information = 0i64;
}
```

在 IRP_MJ_CREATE 迴圈尋找 Disk 的 Device Object

epmntdrv.sys一功能濫用

TEAMT5 杜浦數位安全

```
  v9 = IoBuildAsynchronousFsdRequest(
         3u,
         FsContext_v5,
         MappedSystemVa_v7,
         IoStackLocation_v2->Parameters.Read.Length,
         &Timeout,
         &IoStatusBlock);
  if ( !v9 )
  {
LABEL_8:
    v8 = -1073741670;
    goto LABEL_22;
  }
  KeInitializeEvent(&Event, NotificationEvent, 0);
  v10 = v9->Tail.Overlay.CurrentStackLocation;
  v10[-1].CompletionRoutine = (PIO_COMPLETION_ROUTINE)&sub_11380;
  v10[-1].Control = -32;
  v10[-1].Context = &Event;
  v8 = IofCallDriver(FsContext_v5, v9);
```

呼叫 Disk 的 IRP_MJ_READ

epmntdrv.sys一功能濫用

TEAMT5 杜浦數位安全

```
v11 = IoBuildAsynchronousFsdRequest(4u, FsContext_v5, v7, v10, &Timeout, &IoStatusBlock);
if ( v11 )
{
  KeInitializeEvent(&Event, NotificationEvent, 0);
  v12 = v11->Tail.Overlay.CurrentStackLocation;
  v12[-1].CompletionRoutine = (PIO_COMPLETION_ROUTINE)&sub_11380;
  v12[-1].Control = -32;
  v12[-1].Context = &Event;
  v8 = IofCallDriver(FsContext_v5, v11);
```

呼叫 Disk 的 IRP_MJ_WRITE

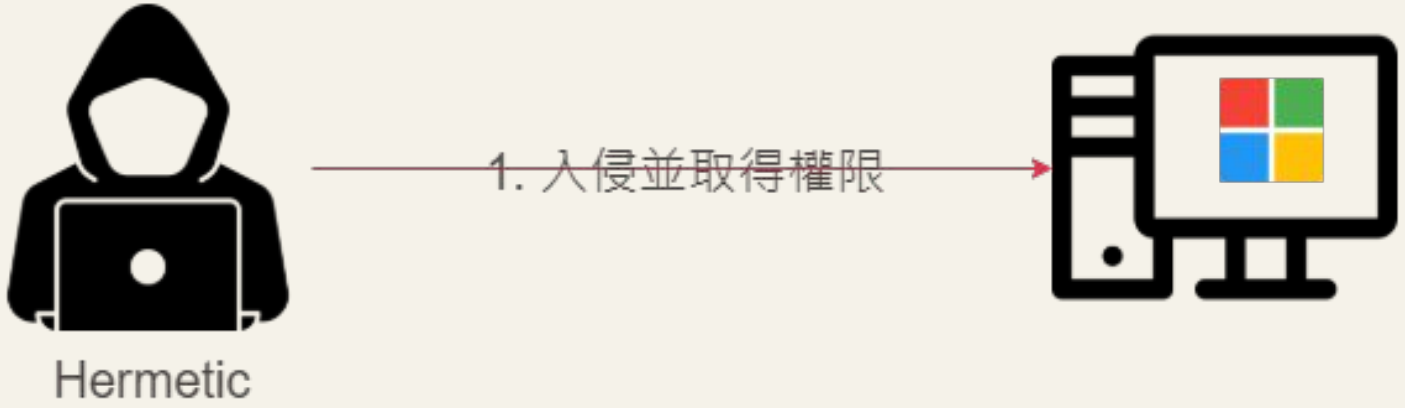
epmntdrv.sys一功能濫用

TEAMT5 杜浦數位安全

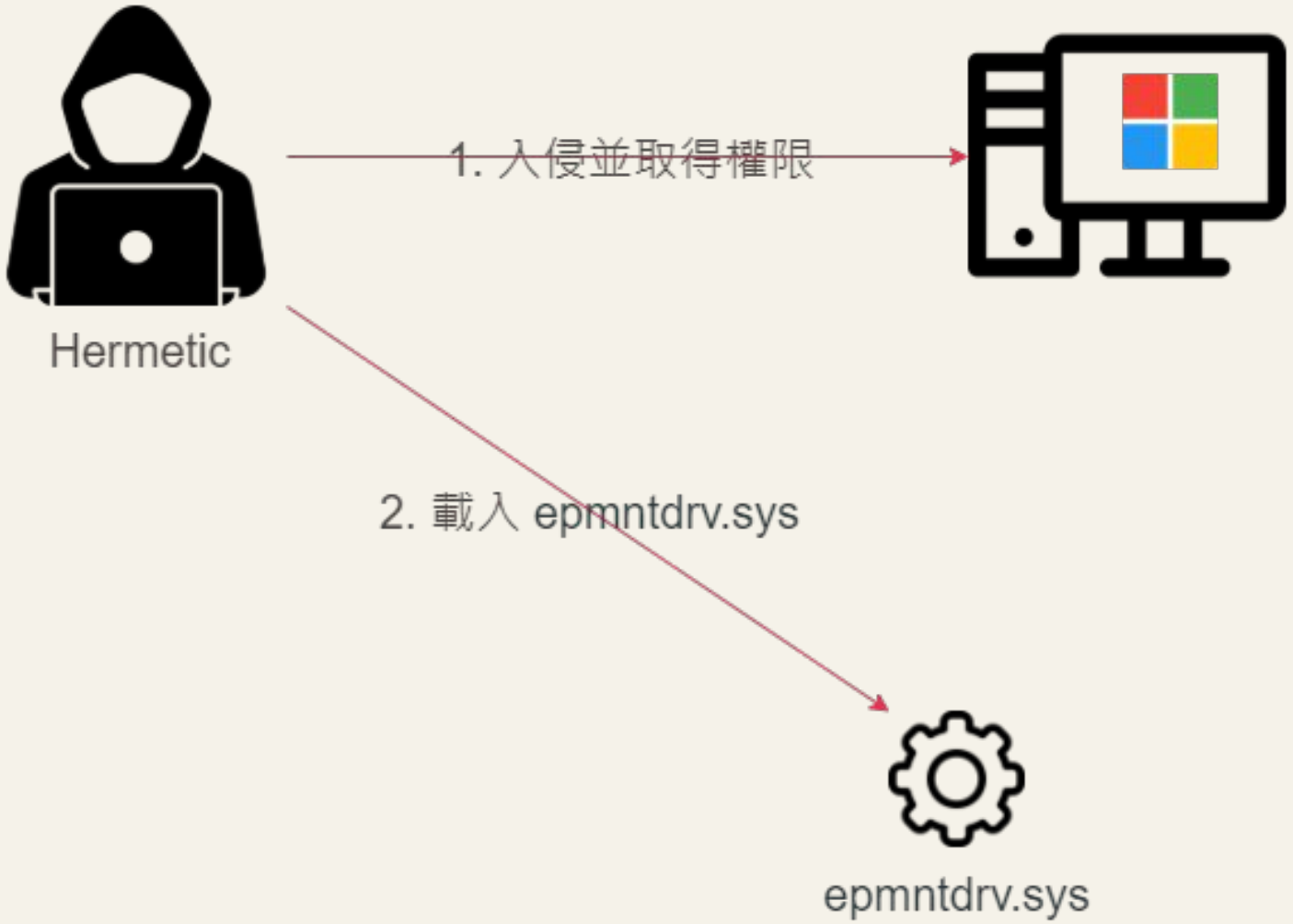
```
v6 = IoGetAttachedDeviceReference(FileContext_v5);
if ( v6 && (OutputBuffer = pIrp_a2->AssociatedIrp.MasterIrp) != 0i64 )
{
  KeInitializeEvent(&Event, NotificationEvent, 0);
  v9 = IoBuildDeviceIoControlRequest(
         IoStackLocation_v2->Parameters.Read.ByteOffset.LowPart,
         v6,
         OutputBuffer,
         IoStackLocation_v2->Parameters.Create.Options,
         OutputBuffer,
         IoStackLocation_v2->Parameters.Read.Length,
         0,
         &Event,
         &IoStatusBlock);
  if ( v9 )
  {
    v7 = IofCallDriver(v6, v9);
    if ( v7 == 259 )
    {
      KeWaitForSingleObject(&Event, Executive, 0, 0, 0i64);
      v7 = IoStatusBlock.Status;
    }
    pIrp_a2->IoStatus.Information = IoStatusBlock.Information;
  }
  else
  {
    v7 = -1073741670;
  }
}
```

呼叫 Disk 的 IRP_MJ_DEVICE_CONTROL

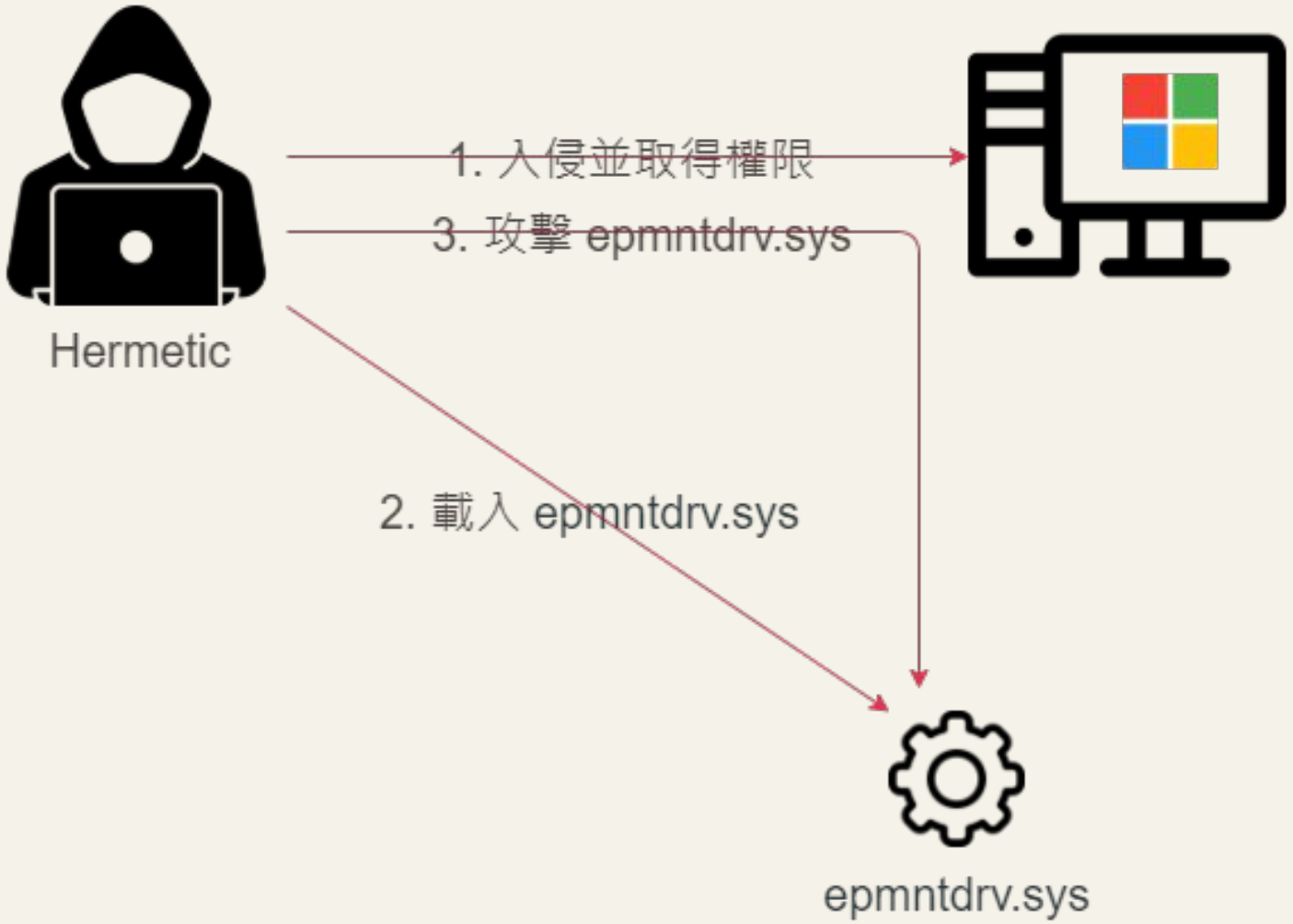
Hermetic－破壞系統



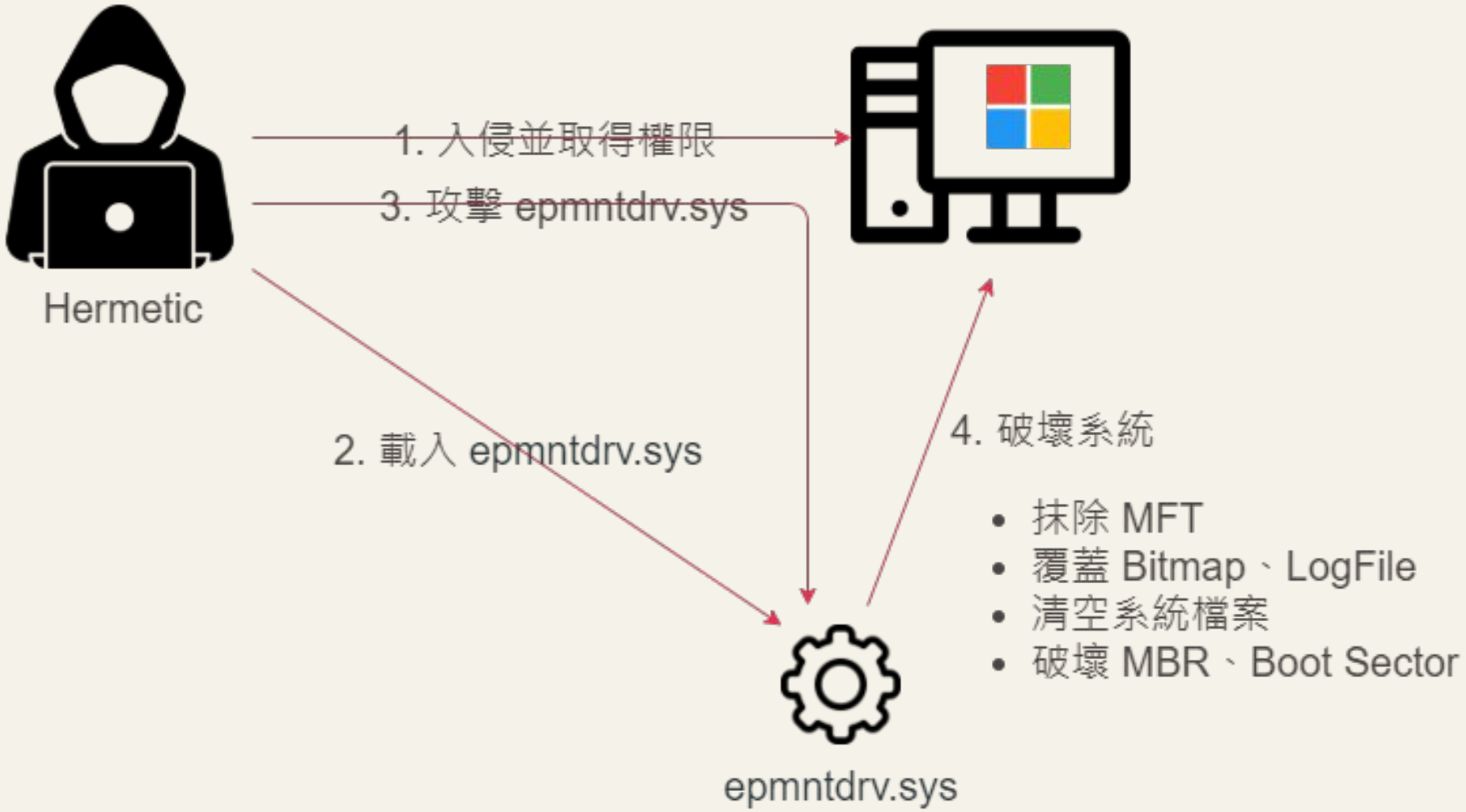
Hermetic－破壞系統



Hermetic－破壞系統



Hermetic－破壞系統



DEMO

改善與防禦

改善與防禦

- 給驅動程式開發者的建議
- 給系管、網管的建議
- 防毒廠商應對措施

給驅動程式開發者的建議

- 用多少做多少
- 檢查存取權限
- 產品的資安檢測

給系管、網管的建議

- 針對 N-Day：引入 Microsoft 建議的驅動程式封鎖規則
- 減少入侵系統的攻擊面，關閉不需要的服務
- 定期備份檔案資料
- 定期更新系統與第三方軟體

防毒廠商的應對措施

- 黑名單可被濫用的驅動程式
- 偵測潛伏的 Kernel Rootkit
- 數位鑑識
- 從攻擊鏈阻斷惡意程式

Conclusion

- BYOVD（Bring Your Own Vulnerable Driver）攻擊濫用有漏洞的第三方驅動程式
- BYOVD 攻擊利用 Kernel 權限更進一步掌控系統
- 開發商、系管與網管、防毒廠商需要有針對此攻擊的應對措施

THANKS FOR LISTENING !

Zeze

zeze@teamt5.org