系統安全組

T5CAMP

鉤進火狐的心

羅崧瑋　劉宜蓁

2025.01.16

INTRO

- Camp上課教的是chrome，想透過了解firefox的實作方式，學習惡意程式開發

- ~~搞人家，投毒到室友電腦~~

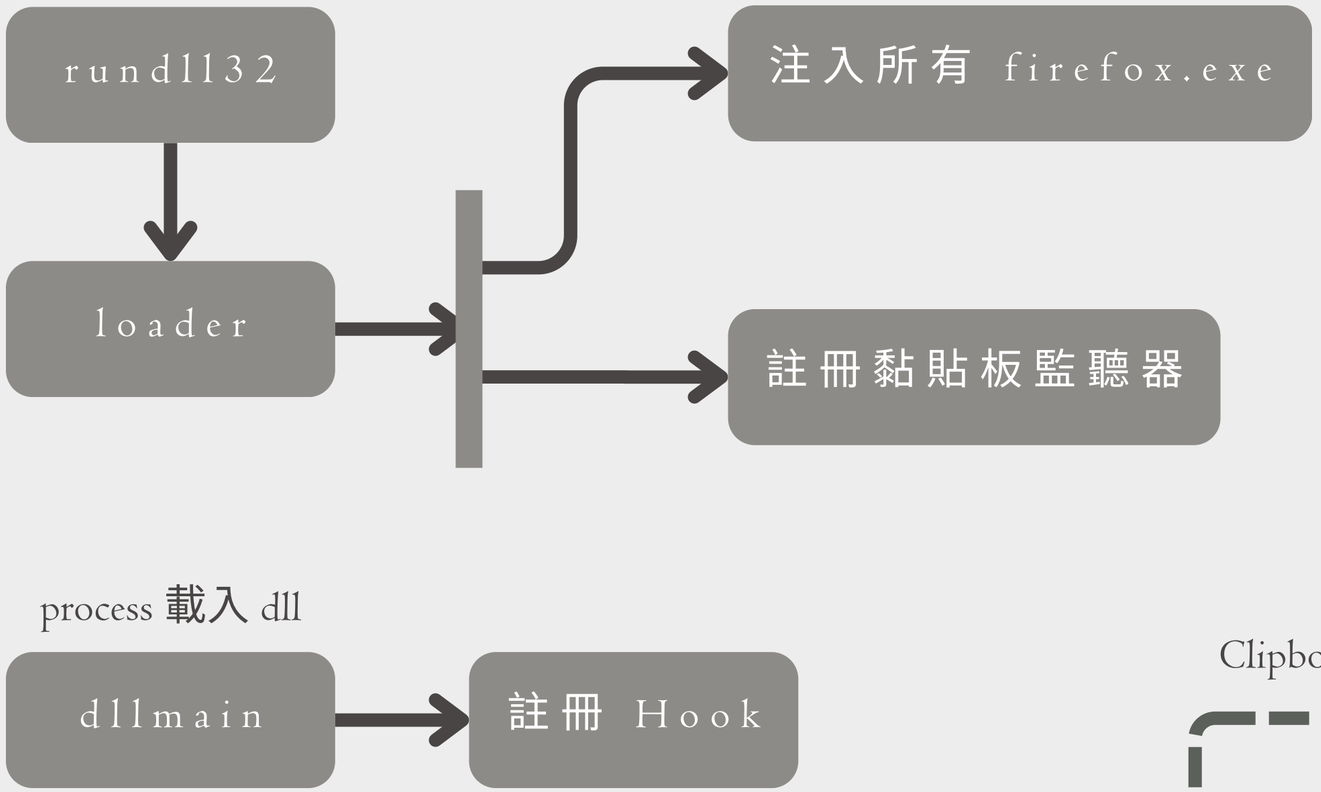
THEME

FIREFOX HOOKER + CLIPPER LOGGER

=HASHING CLIPBOARD DATA

WHILE HOOKING UR WEB :)

FIREFOX HOOKING

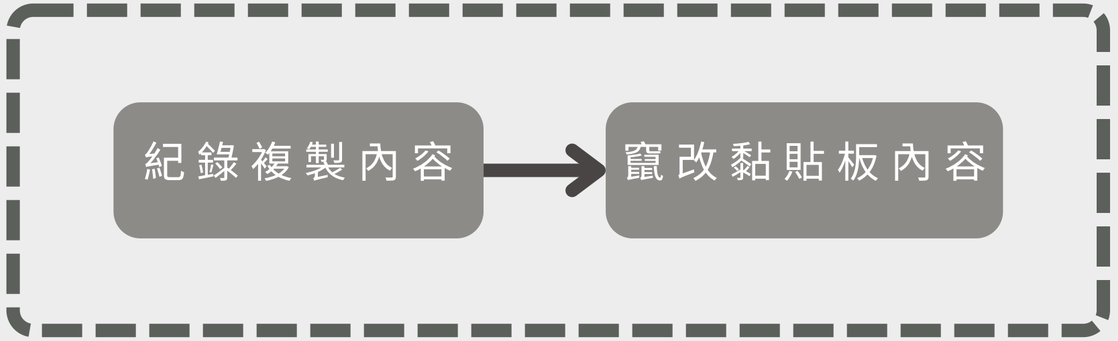


process 載入 dll

HookPR_Write()

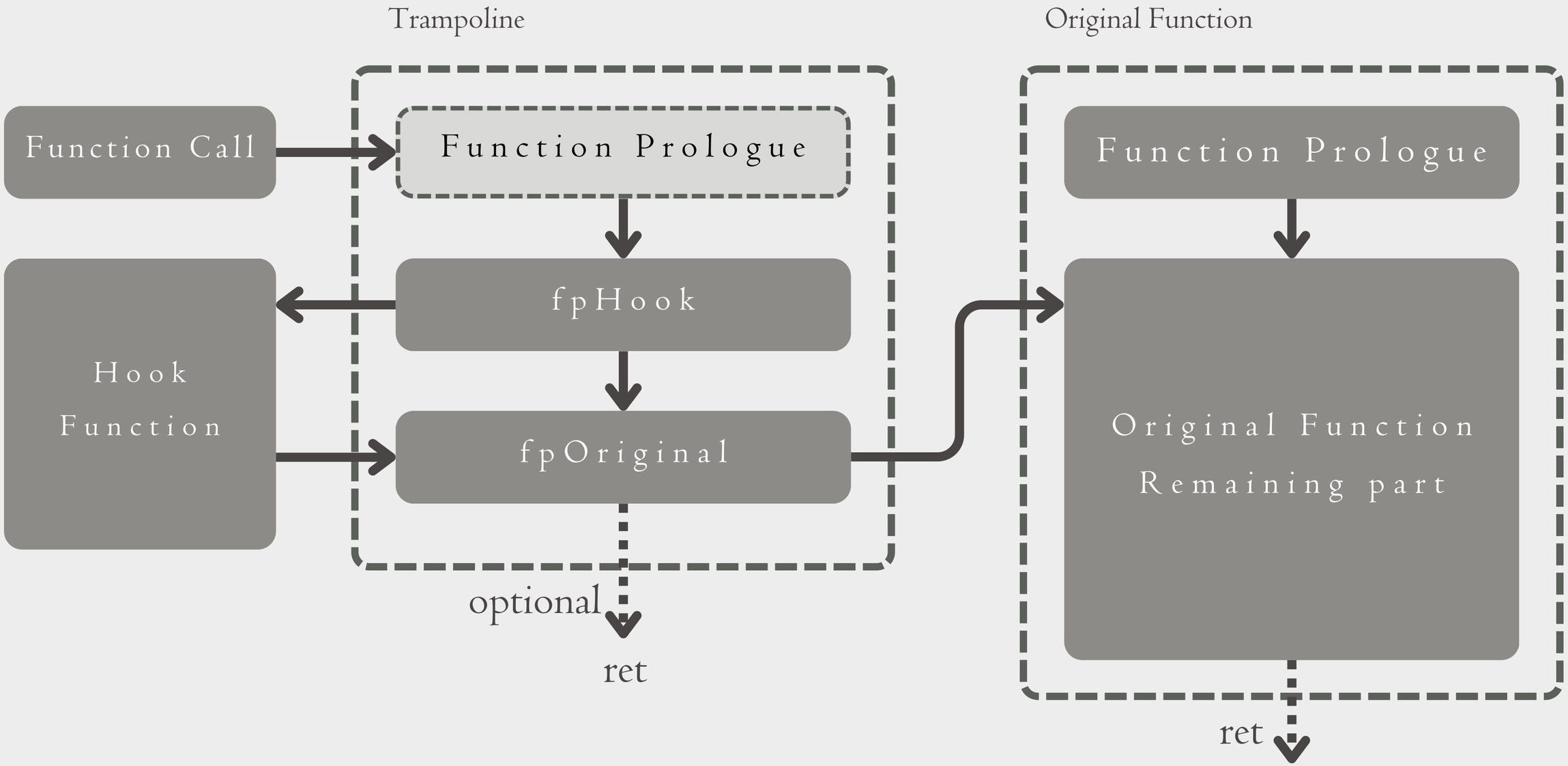
HookPR_Read()

ClipboardViewerProc



HOOKING METHODS

文字

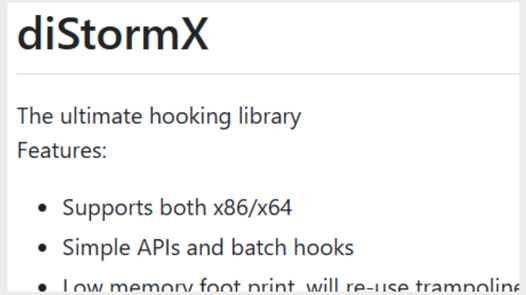


MINHOOK/DISTORMX

第三方程式庫

1.初始化記憶體--MH_Initialize()
2.建立trampoline與entry--MH_CreateHook()
3.修改目標函數-MH_EnableHook()

1. 計算需要的指令長度--GetInstructionLength(自帶B64 decode)
2. 分配 trampoline 空間--VirtualAlloc
3. 複製到記憶體--memcpy
4. 建立 trampoline(jump+total size)
5. 修改目標函數--設置原始函數指標



RELATED DLLS

FIREFOX DYNAMIC LIBRARY

nss3.dll

功能: 處理TLS/SSL相關的證書加密/連線請求

nspr4.dll

功能: 即時網路資料傳輸

發起連接請求

- PR_Connect

接收資料：

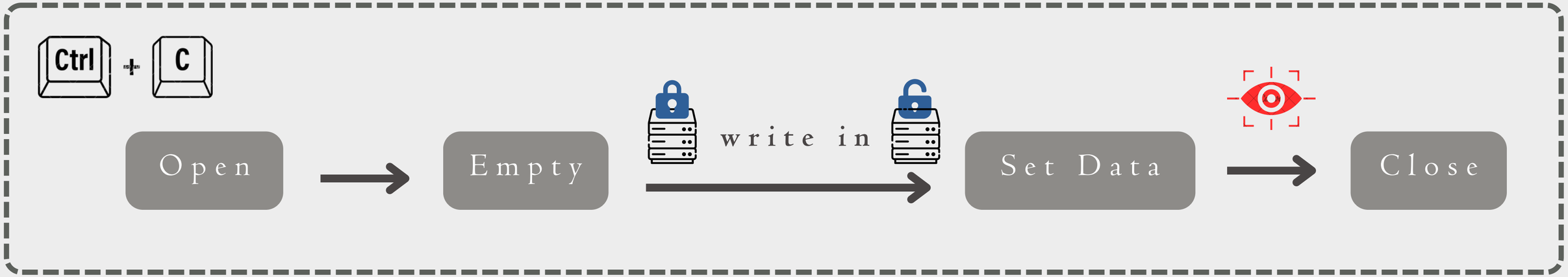
- PR_Read
- PR_Recv

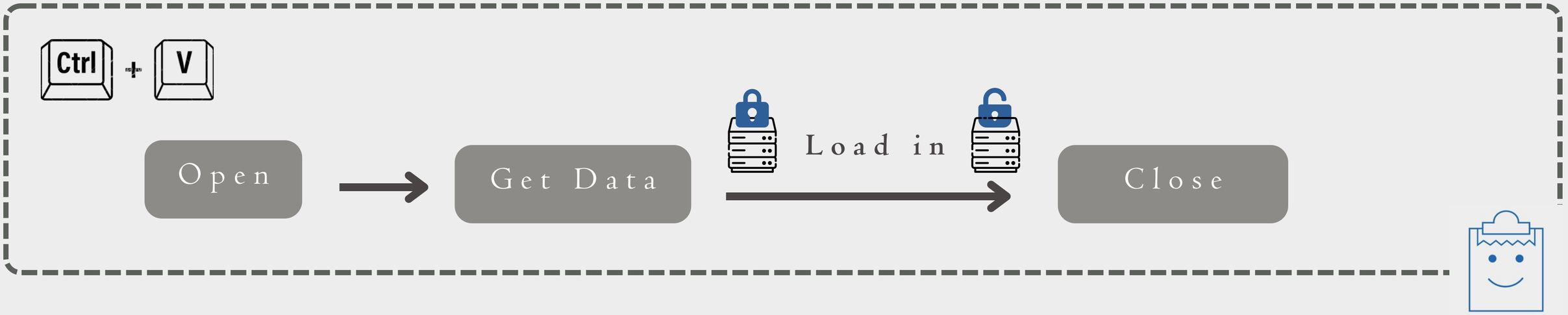
傳送資料：

- PR_Write
- PR_Writev
- PR_Send
- PR_TransmitFile

CLIPBOARD WORKFLOW

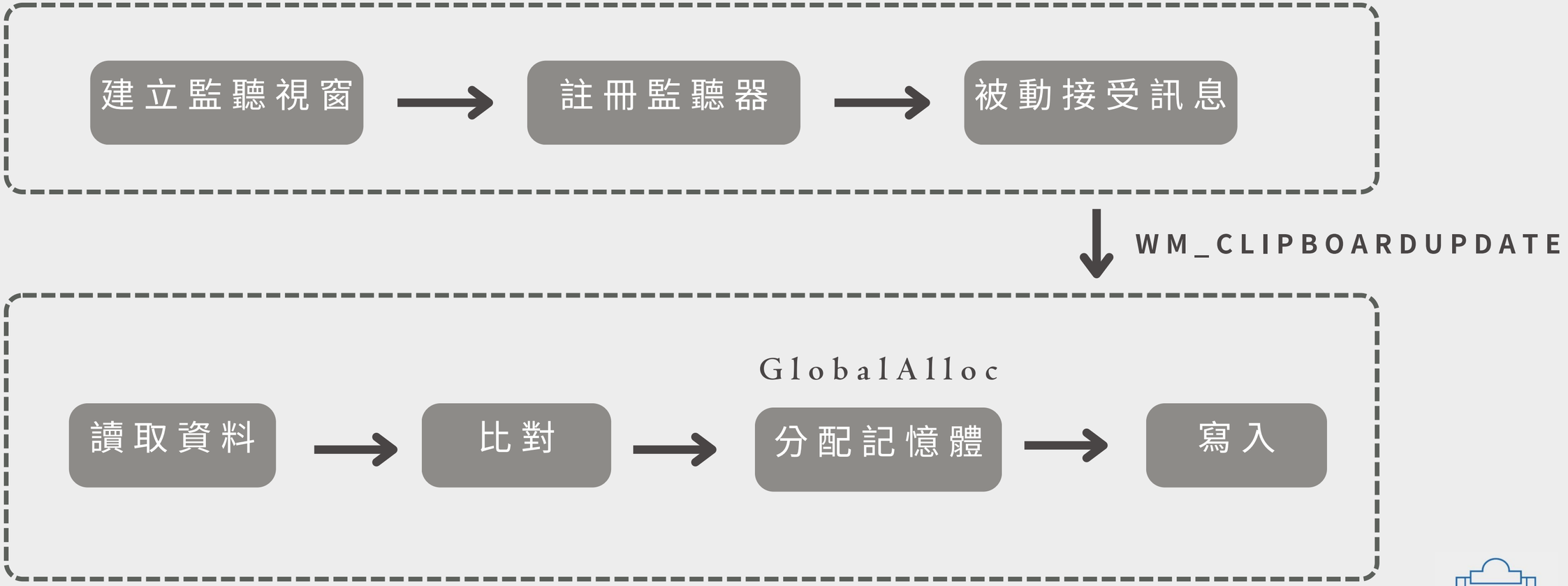
剪貼簿複製/貼上流程





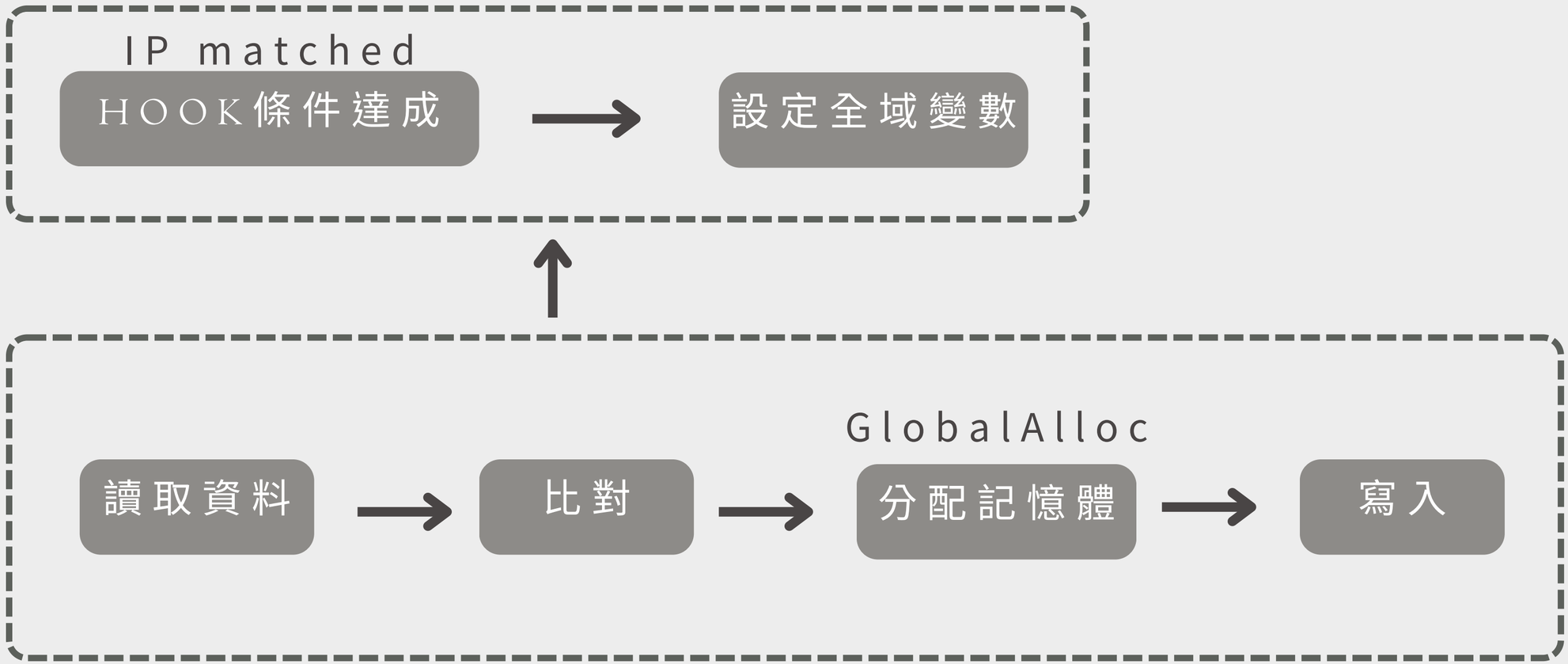
CLIPBOARD TAMPERING

剪貼簿竄改



CLIPBOARD TAMPERING

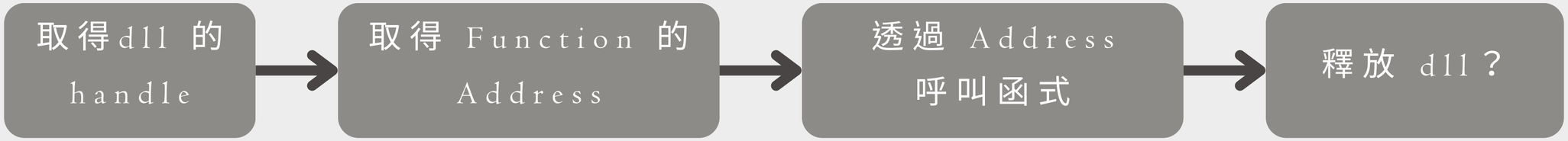
剪貼簿竄改



DYNAMIC LOADING

函式的動態載入

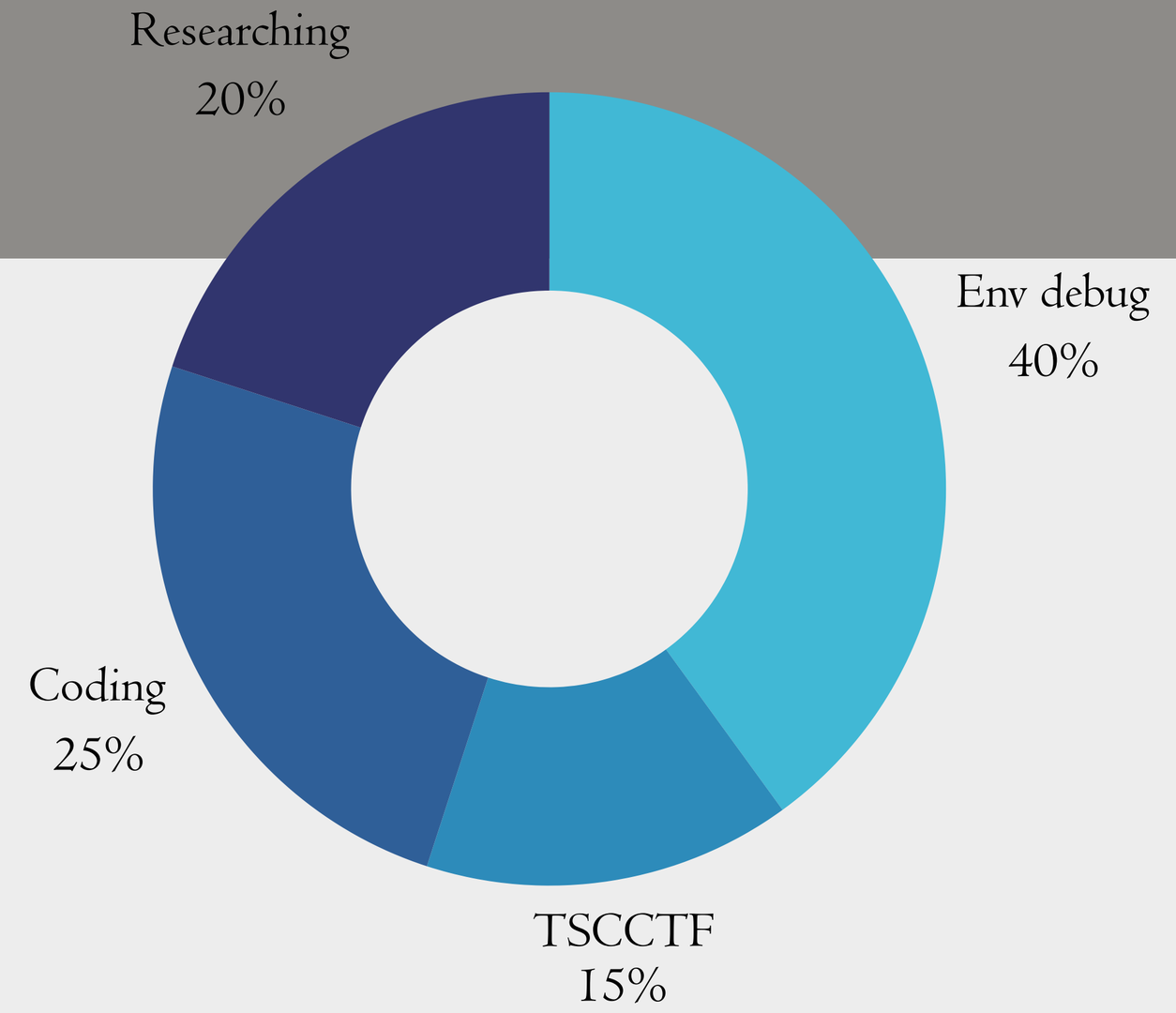
- 避免出現在 Import Address Table
- 增加分析難度？



TEXT
文字

FEEDBACK

心得與感想



DEMO

TeamT5 杜浦數位安全 - Persist

https://teamt5.org/tw/

企業資安防禦的關鍵點：暗網情資>>>立即了解>>>

TEAMT5

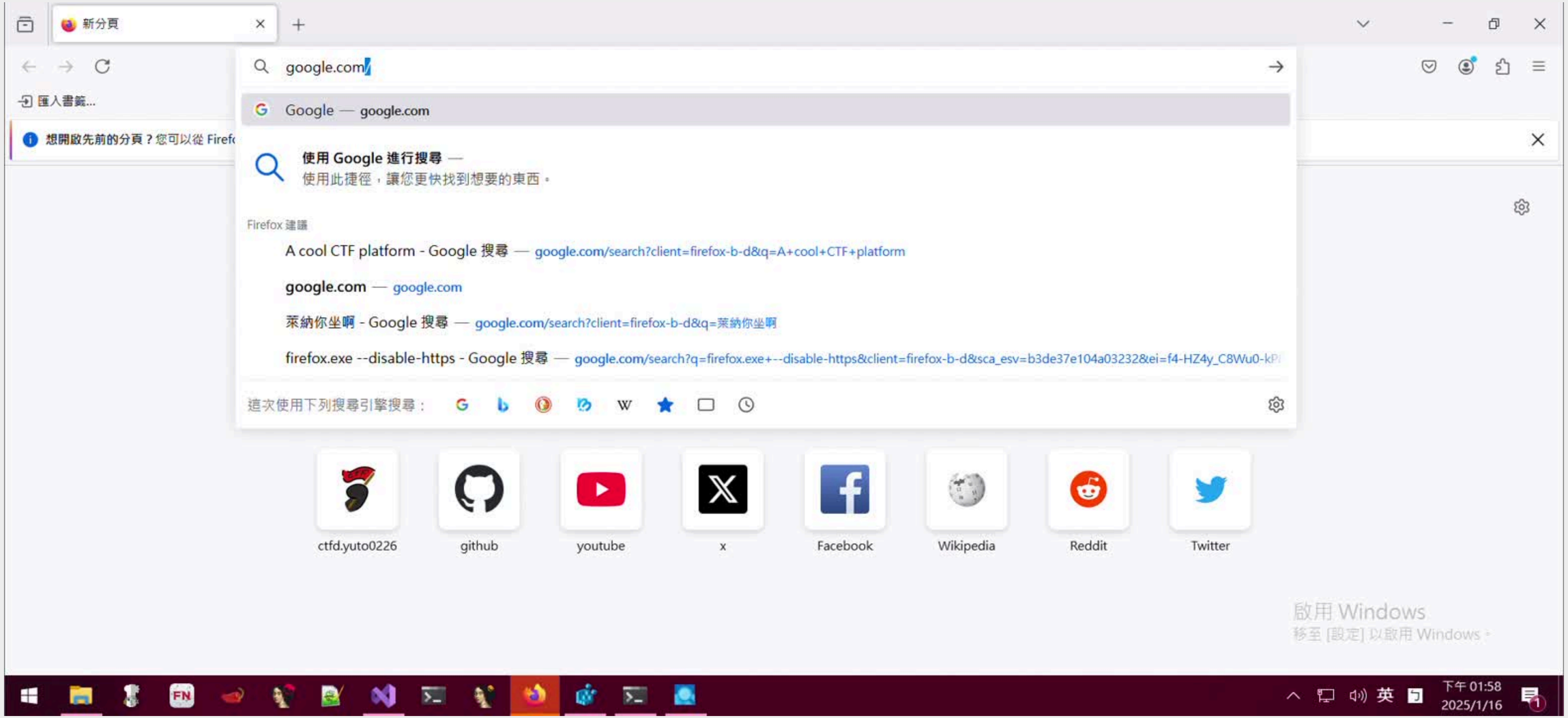
服務 產品 產業方案 關於 TeamT5 最新消息 部落格 聯絡我們 TW

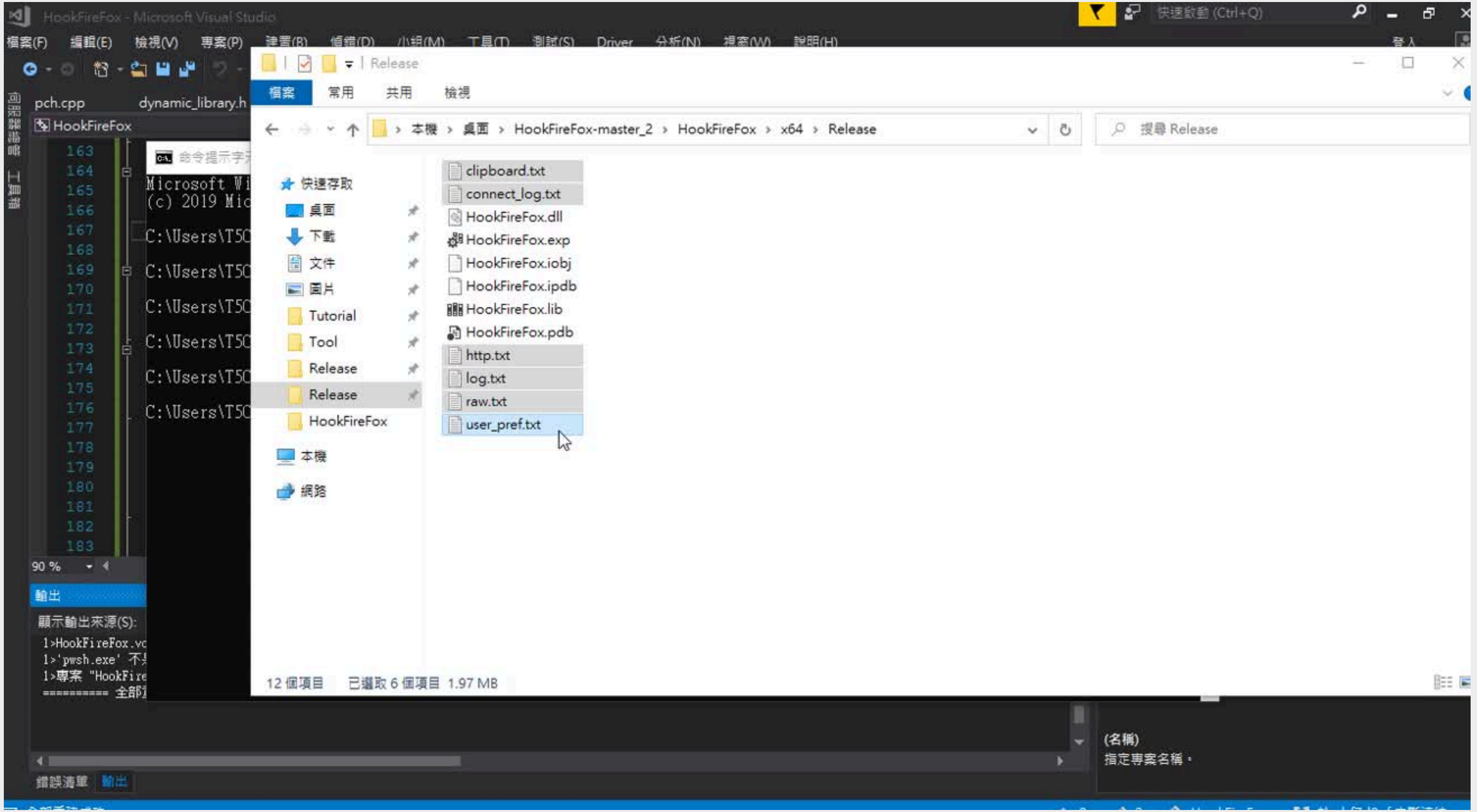
情資驅動資安防禦

我們堅持威脅情資是資安防禦的基石，為企業提供行動取向的在地情資，協助企業預見攻擊，提前部署防禦策略，降低損失風險。

了解更多

聯絡我們


新分頁
匯入書籤...
想開啟先前的分頁？您可以從 Firefo
google.com
Google — google.com
使用 Google 進行搜尋 —
使用此捷徑，讓您更快找到想要的東西。
Firefox 建議
A cool CTF platform - Google 搜尋 — google.com/search?client=firefox-b-d&q=A+cool+CTF+platform
google.com — google.com
萊納你坐啊 - Google 搜尋 — google.com/search?client=firefox-b-d&q=萊納你坐啊
firefox.exe --disable-https - Google 搜尋 — google.com/search?q=firefox.exe+--disable-https&client=firefox-b-d&sca_esv=b3de37e104a03232&ei=f4-HZ4y_C8Wu0-kP
這次使用下列搜尋引擎搜尋：
ctfd.yuto0226
github
youtube
x
Facebook
Wikipedia
Reddit
Twitter
啟用 Windows
移至 [設定] 以啟用 Windows。
英
下午 01:58
2025/1/16


HookFireFox - Microsoft Visual Studio
檔案(F) 編輯(E) 檢視(V) 專案(P) 建置(B) 偵錯(D) 小組(M) 工具(T) 測試(S) Driver 分析(N) 視窗(W) 說明(H)
快速啟動 (Ctrl+Q)
登入
pch.cpp
dynamic_library.h
HookFireFox
Release
檔案 常用 共用 檢視
本機 › 桌面 › HookFireFox-master_2 › HookFireFox › x64 › Release
搜尋 Release
快速存取
桌面
下載
文件
圖片
Tutorial
Tool
Release
Release
HookFireFox
本機
網路
clipboard.txt
connect_log.txt
HookFireFox.dll
HookFireFox.exp
HookFireFox.iobj
HookFireFox.ipdb
HookFireFox.lib
HookFireFox.pdb
http.txt
log.txt
raw.txt
user_pref.txt
12 個項目 已選取 6 個項目 1.97 MB
C:\Users\T5C
90 %
輸出
顯示輸出來源(S):
1>HookFireFox.vc
1>'pwsh.exe' 不是
1>專案 "HookFire
========== 全部建
(名稱)
指定專案名稱。
錯誤清單 輸出

REFERENCE

現實主義勇者的 WINDOWS 攻防記 系列

FIREFOX-GRABBER

NADIR, I., AHMAD, Z., MAHMOOD, H., SHAH, G.A., SHAHZAD, F., UMAIR, M., KHAN, H., GULZAR, U.: AN AUDITING FRAMEWORK FOR VULNERABILITY ANALYSIS OF IOT SYSTEM. IN: 2019 IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY WORKSHOPS (EUROS &PW), PAGES 39–47. IEEE (2019)