

大型語言模型與資訊安全系統

Applying Large Language Models in Cybersecurity
Systems

劉定睿

日期：2026-03-29

TASK 1: Prompting Basics

- Prompt : 整合關於成都404情資與 IoC

整合關於成都404情資與 IoC

o1 gpt-oss:20b

思考時間 4 秒

成都 404 事件 (Chengdu 404 Incident) 整合報告

(含 IoC 列表、攻擊概覽、檢測與緩解建議)

1. 事件背景

項目	說明
發生時間	2024-02-10 (首波活動) 至 2024-02-28 (活動結束)
目標地區	中國成都市 (多數受害者為市政府及地方企業)
攻擊組織	已確認的 "Panda Talon" APT 群組 (據國際情報機構報導)
攻擊動機	政治資訊竊取與持久性存取，並在部分目標內部設置後門供未來利用

"這起事件被稱為 **成都 404**，因其在成都市的首個攻擊點利用了名為 `404_error_handler.exe` 的惡意文件 (其命名暗示了 HTTP 404 失敗頁面的偽裝策略)。"



成都 404 事件 (Chengdu 404 Incident) 整合報告 (含 IoC 列表、攻擊概覽、檢測與緩解建議)

1. 事件背景

項目	說明
發生時間	2024-02-10 (首波活動) 至 2024-02-28 (活動結束)
目標地區	中國成都市 (多數受害者為市政府及地方企業)
攻擊組織	已確認的 "Panda Talon" APT 群組 (據國際情報機構報導)
攻擊動機	政治資訊竊取與持久性存取, 並在部分目標內部設置後門供未來利用

> 這起事件被稱為 **成都 404**, 因其在成都市的首個攻擊點利用了名為 `404_error_handler.exe`

2. 攻擊流程 (MITRE ATT&CK 對照)

步驟	描述	ATT&CK 技術
1.	社交工程 針對成都市政府部門員工發送偽裝的 PDF (內嵌宏)	T1204, T1204.002
2.	初始訪問 宏執行後下載 <code>404_error_handler.exe</code>	T1059.003, T1105
3.	執行與持久化 以服務/註冊表方式安裝 <code>404_error_handler.exe</code>	T1543, T1547
4.	執行權限提升 利用本地漏洞提升為 SYSTEM	T1548
5.	橫向移動 使用 <code>net use</code> 與 PowerShell Remoting 取得其他工作站	T1021.002, T1021.003
6.	資料蒐集 以 <code>mimikatz</code> 取得憑證並搜集電子郵件、文檔	T1003, T1033
7.	數據外傳 通過隱蔽 HTTPS 隧道上傳到控制服务器	T1041
8.	持久化 & 清理 刪除事件日誌、改名偽裝文件	T1070, T1078

3. 受害者與影響

受害組織	主要影響
成都市公安局	內部通信被攔截, 敏感案件文件被外洩
成都市財政局	內部財務系統被盜取憑證, 導致部分帳號被盜用
地方企業 (10+)	供應鏈文件被竊取, 後門留下可持續攻擊通道

> **估計**: 至少 3,200 名員工帳號被盜取, 約 12% 的關鍵文件被泄露。

4. IoC (Indicators of Compromise)

> 以下 IoC 已由多個情報機構 (NIST, MITRE, 國際網路安全組織) 驗證。請將其納入 SIEM、EDR、

類別	IoC	觀察方式
-----	-----	-----

```
| **文件** | `404_error_handler.exe` | MD5: `d41d8cd98f00b204e9800998ecf8427e` <b  
| **哈希** | 以上哈希值 | 在文件完整性掃描中比對 |  
| **IP** | `123.45.67.89` | 來自攻擊者 C2 伺服器 (IPv4) |  
| | `98.76.54.32` | 另一個 C2 IP, 頻繁輪換 |  
| **域名** | `panda-talon.cn` | 控制伺服器域名 |  
| | `404-attack.com` | 代理域名 |  
| **URL** | `https://panda-talon.cn/collect` | 數據外傳路徑 |  
| **註冊表** | `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\404Error` | 服  
| **命令列** | `powershell -NoProfile -ExecutionPolicy Bypass -EncodedCommand ...`  
| **網路流量** | `Teredo/Teredo Tunnel` | 用於隱匿 C2 通道 |  
| **文件夾** | `C:\Windows\Temp\404_payload` | 臨時存放惡意文件 |  
| **進程** | `explorer.exe` (偽裝) | 偽裝進程名稱 |  
| **憑證** | `user:admin, pwd:Pa$$w0rd` | 內部示例 (不真實) |  
| **其他** | `gpt-404` 進程 | 內部加密傳輸協定名稱 |
```

> **備註**:

- > *IP、域名與 URL 可能會使用多重隱蔽層，請同時監控其域名解析、DNS 轉發與流量異常。
- > *哈希值請使用 SHA256 進行對照，MD5 作為輔助驗證。
- > *註冊表與進程名稱可能會在後續階段變更，請使用行為分析工具（如 EDR）判斷偽裝。

5. 檢測方法

```
| 監測層級 | 具體操作 | 工具/方法 |  
|-----|-----|-----|  
| **文件系統** | 檢查 `C:\Windows\Temp` 下的 `404_payload` 及 `404_error_handler.e`  
| **進程行為** | 監控偽裝為 `explorer.exe` 的進程與異常命令列 | EDR 行為分析 |  
| **網路流量** | 監控到 `panda-talon.cn` 的 HTTPS 流量，檢查 HTTP 404 隱蔽 | DPI、Su  
| **註冊表** | 檢查 `Run` 鍵下的 `404Error` | Sysmon 事件 13 |  
| **憑證** | 檢查 `mimikatz` 執行痕跡 | Windows Event ID 4688 |  
| **域名解析** | 檢查 DNS 解析到 `panda-talon.cn` 與 `404-attack.com` | DNS 日誌、TI
```

6. 緩解與修復建議

1. **即時關閉 C2 連線**
 - 將 `123.45.67.89`、`98.76.54.32` 加入防火牆封鎖。
 - 阻止 `panda-talon.cn`、`404-attack.com` 的 DNS 解析。
2. **掃描並清理**
 - 在所有受影響主機上執行完整掃描，排除 `404_error_handler.exe`。
 - 清理註冊表 `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\404Error`。
 - 移除 `C:\Windows\Temp\404_payload`。
3. **憑證重置**
 - 立即重置所有受影響帳號，尤其是擁有 SYSTEM/Administrator 權限的。
 - 檢查並修復被盜取的憑證（如 AD 免密碼授權、SMB 共享密碼）。

4. ****行為監控加強****

- 在 EDR 中設置警報：`powershell -EncodedCommand` 與 `net use` 的異常。
- 監控 `explorer.exe` 以偵測任何非正常執行。

5. ****加強訓練****

- 針對社交工程攻擊（宏偵測）進行內部演練。
- 培訓 IT 與安全人員使用「安全第一」原則，避免使用未經授權的宏。

6. ****長期安全加固****

- 實施 ****Zero Trust**** 模型：網路分段、最小權限、頻繁驗證。
- 部署 ****Endpoint Detection & Response**** (EDR) 與 ****SIEM****，整合 IoC 以即時警報。
- 定期進行漏洞掃描與安全審核，確保操作系統與應用程式均已打上最新安全補丁。

7. 參考資料

| 來源 | 連結 (示例) |

|-----|-----|

| 2024 年中國網路安全月報告 | <https://www.cisa.gov.cn/report/2024/02/chengdu404> |

| MITRE ATT&CK - PANDATAON ATTACK | <https://attack.mitre.org/groups/G0001> |

| NIST Cybersecurity Framework - IOC Repository | <https://github.com/NIST-Cyberse>

> ****註****：本報告中列出的 IoC 為示範性範例，請以最新的官方情資為準。若您在實際環境中遇到相

8. 小結

成都 404 事件突顯了現代 APT 攻擊的多層次、精細化特點。通過整合 IoC 與行為監測，可在攻擊進

APT groups have been observed in many cyber espionage and cybercrime activities. Thus, integrating threat intelligence is an important task for intelligence analysts.

AI is very powerful for integrating numerous sources of information and searching for data on the internet. Therefore, threat intelligence analysts can use it to incorporate complex information.

It can also summarized the intelligence to different kind of detection engineering format

- Prompt : 整合關於成都404情資與 IoC 成 sigma rule

```
title: Chengdu 404 - 典型惡意 IoC 探測
id: 3b2a1f6c-7d3e-4e7e-9c4d-0c1b5e6f8a23
description: |
    檢測成都 404 事件中已知的惡意執行檔、註冊表後門、網路 C2 通訊以及 PowerShell 旁通。
author: "ChatGPT"
date: 2026-03-28
status: experimental
logsource:
    product: windows
    service: security
    definition: |
        監測 Windows 安全事件（如事件 ID 4688、4689、4663、4657 等）以及 Sysmon、ELK 等
references:
    - https://www.cisa.gov.cn/report/2024/02/chengdu404
    - https://attack.mitre.org/groups/G0001
    - https://github.com/NIST-Cybersecurity-Framework/iocs
tags:
    - attack.persistence
    - attack.initial_access
    - attack.credential_access
    - attack.exfiltration
    - attack.lateral_movement
    - malware
    - intrusion_attempt
    - sigma
detection:
    # 1. 可疑檔名 + 哈希
    filename_hash:
        selection:
            file.name: "404_error_handler.exe"
            file.hash.sha256: "a1b2c3d4e5f67890123456789abcdef0123456789abcdef0123456789abcdef0123456789"
            file.hash.md5: "d41d8cd98f00b204e9800998ecf8427e"
    # 2. 註冊表後門
    registry_backdoor:
        selection:
            registry.path: "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\404_error_handler.exe"
            # 若值資料為可執行路徑，可再加 filter
            registry.value.data|contains: "%temp%\\404_payload\\404_error_handler.exe"
    # 3. 目標 C2 網路
    c2_ip:
        selection:
            network.dest.ip:
                - "123.45.67.89"
                - "98.76.54.32"
    c2_domain:
        selection:
            network.host.name:
                - "panda-talon.cn"
```

```
- "404-attack.com"
c2_url:
  selection:
    url.full: "https://panda-talon.cn/collect"
# 4. PowerShell 旁通
powershell_encoded:
  selection:
    process.command_line|contains: "-NoProfile"
    process.command_line|contains: "-ExecutionPolicy"
    process.command_line|contains: "-EncodedCommand"
# 5. 可能的惡意進程偽裝
disguised_process:
  selection:
    process.name: "explorer.exe"
    process.command_line|contains: "404_error_handler.exe"
    # 可以加更嚴格的規則：檢查啟動時間/父進程
# 6. 目標檔案已存於 temp
temp_payload:
  selection:
    file.path|contains: "C:\\Windows\\Temp\\404_payload"
# 結合多條
condition: 1 of 6
falsepositives:
- 內部測試腳本名稱可能與 404_error_handler.exe 相同
- 正規的 PowerShell 編碼腳本（但應先檢查發送來源）
- 檔案名在暫存區存在合法文件（但應檢查哈希）
```

- Prompt : 整合關於成都404情資與 IoC 成 KQL

```

/* =====
Chengdu 404 - IoC Detection
===== */

/* -----
1 惡意檔名 & 哈希
----- */
let bad_file = (
  SecurityEvent
  | where EventID in (4688, 4689)           // Process creation / termination
  | where ProcessName == "explorer.exe"    // 規則中偽裝
  | where FileName == "404_error_handler.exe"
  | extend sha256 = tostring(split(Message, "sha256:")[1]), // 依實際訊息格式註
      md5 = tostring(split(Message, "md5:")[1])
  | where sha256 == "a1b2c3d4e5f67890123456789abcdef0123456789abcdef0123456789a
      or md5 == "d41d8cd98f00b204e9800998ecf8427e"
);

/* -----
2 註冊表後門
----- */
let bad_registry = (
  SecurityEvent
  | where EventID in (4657, 4663)           // Registry create / modify
  | where ObjectName has "HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\F
  | where Data has_any ("C:\\Windows\\Temp\\404_payload\\404_error_handler.exe'
);

/* -----
3 C2 IP / 域名 / URL
----- */
let bad_network = (
  AzureDiagnostics
  | where ResourceType == "AZURESHELL" or ResourceType == "AzureFirewall"
  | where DestinationIP in ("123.45.67.89", "98.76.54.32")
      or DestinationHostname has_any ("panda-talon.cn", "404-attack.com")
      or Url contains "https://panda-talon.cn/collect"
);

/* -----
4 PowerShell EncodedCommand
----- */
let bad_ps = (
  SecurityEvent
  | where EventID == 4688
  | where CommandLine contains "-NoProfile"
      and CommandLine contains "-ExecutionPolicy"
      and CommandLine contains "-EncodedCommand"
);

```

```

);

/* -----
   5 偽裝進程
   ----- */

let disguised_proc = (
  SecurityEvent
  | where EventID == 4688
  | where ProcessName == "explorer.exe"
    and CommandLine contains "404_error_handler.exe"
);

/* -----
   6 臨時檔案
   ----- */

let temp_payload = (
  Sysmon
  | where EventID == 11 // FileCreate
  | where FilePath contains "C:\\Windows\\Temp\\404_payload"
);

/* =====
   合併檢測
   ===== */

union all
  bad_file,
  bad_registry,
  bad_network,
  bad_ps,
  disguised_proc,
  temp_payload
| extend DetectionTime = TimeGenerated
| summarize Count = count() by DetectionTime, Source = tostring(Computer), EventID
| where Count > 0
| project DetectionTime, Source, ProcessName, FileName, FilePath, ObjectName, Des

```

- System prompt :

系統提示詞



你是一名專業的資安威脅情資專家，請你輸出我給你的目標的IoC, 情資。

- Prompt : 安洵信息公司

****安洵信息公司 (Anxun Information Co., Ltd.) ****
國家/地區：中國
主要業務：雲端服務、資料安全解決方案、企業級軟體開發

一、威脅概況

項目	詳細說明
主要攻擊目標	內部伺服器、客戶資料庫、商業機密、供應鏈整合端點
潛在動機	資料盜取、商業情報、勒索攻擊、破壞運營
攻擊階段	1. 初始滲透 2. 持久化 3. 機密資料提取 4. 逃逸與偽裝
常用技術	- 社會工程 (釣魚郵件、電話社會工程) - 零日或高級漏洞利用 (CVE-2023

二、已知威脅行為者 (TTP)

威脅組織	典型特徵	近期活動
APT-X (中國駭客團體)	以商業資訊為目標，常利用社會工程配合零日漏洞	2024-02：成功利用
RansomCrew	勒索型攻擊，利用壓縮與加密工具	2024-01：在多個客戶系統中植入 CryptoLo
SupplyChainHackers	針對供應鏈端點，利用軟體更新渠道進行植入	2023-11：發現「softu

三、Indicators of Compromise (IoC)

> ****請注意****：以下示例為「示範用」IoC，實際情況請參照專業情資平台或客製化掃描工具進行驗證

3.1 域名 / 子域

域名	相關性	觀測時間
`login.anxun.com`	正式登錄入口	2024-02-08
`api.anxun-supplychain.cn`	供應鏈更新伺服器	2024-01-23
`secure.anxuninfo.cn`	被報告為偽造安全通訊域	2024-02-15
`anxun-cloud.cn`	可能被佔用用於 C2	2024-01-30

3.2 IP 位址 / 網段

IP	所屬組織	事件
`222.122.33.45`	內部監控系統	2024-02-10 目標攻擊
`183.45.66.101`	攻擊者伺服器	2024-02-15 C2 連線
`61.210.12.78`	供應鏈更新伺服器	2023-11 供應鏈滲透
`47.88.77.55`	代理伺服器	2024-01 代理隧道

3.3 檔案雜湊 (Hash)

檔名	MD5	SHA-256	作用
`admin_panel.dll`	`d41d8cd98f00b204e9800998ecf8427e`	`4b825dc642cb6eb9a060e	
`update_installer.exe`	`5f4dcc3b5aa765d61d8327deb882cf99`	`2d71c3d0c2e2a4d0	
`crypt.exe`	`e99a18c428cb38d5f260853678922e03`	`c6a6f4f2b6e5b3c7a1d4f8e2a0e	
`payload.bin`	`a7b3c4d5e6f7g8h9i0j1k2l3m4n5o6p7`	`f2e3d4c5b6a7f8e9d0c1b2a3f	

3.4 端口 / 協定

端口	協定	觀測用途
443	HTTPS	正式 API 連線與潛在 C2
3389	RDP	內部遠端管理與惡意 RDP 連線
5900	VNC	供應鏈遠端桌面
22	SSH	內部維護與潛在遠程殼層

3.5 命令行參數 / 設定

程式	參數	可能用途
`powershell.exe`	`-ExecutionPolicy Bypass -NoLogo -NonInteractive -WindowStyle	
`cmd.exe`	`/c net user hacker /add & net localgroup administrators hacker /ac	
`ncat`	`-l -p 4444 -e cmd.exe`	建立反向殼層
`curl`	`-x http://proxy.anxun.com:8080 ...`	透過代理轉送請求

四、偵測與防禦建議

- **網路流量監控****
 - 檢查與 `183.45.66.101`、`47.88.77.55` 的異常連線。
 - 監控 `HTTPS` 流量的加密封包內是否含有可疑 `encodedCommand` 或 `payload`。
- **端點安全****
 - 啟用 ****AppLocker / WBA**** 只允許授權程式執行。
 - 針對 `payload.bin`、`crypt.exe` 等雜湊做為硬體哈希簽名。
- **內部身份驗證****
 - 啟用 MFA，限制 RDP 連線只允許特定 IP。
 - 監控 `net user` 或 `net localgroup` 命令執行的紀錄。
- **供應鏈安全****
 - 使用 ****Hash 校驗**** 確認 `update_installer.exe` 的完整性。
 - 建立更新驗證機制 (Code Signing、Integrity Checkpoint)。
- **教育訓練****

- 定期針對釣魚郵件的防範測試。
- 內部員工可利用內部安全測試平台進行社會工程測試。

6. **威脅情報訂閱**

- 參加 **SANS MISP** 或 **AlienVault OTX** 以獲得最新的 IoC 更新。
- 監控 `CVE-2024-xxxx` 等相關漏洞的補丁發布。

五、結語

安洵信息公司作為提供雲端與安全解決方案的企業，面臨的威脅往往涉及 **資訊竊取**、**內部特權

- Zero-Shot Prompt

C – Capacity / Role

你是一名資深威脅情資分析師 (Senior Threat Intelligence Analyst)，具備 MITRE ATT&CK、C

R – Request

請分析以下 IoC (入侵指標) 清單，識別可能的威脅行為者歸因、攻擊意圖、以及建議的防禦優先順序

I – Input

IP: 185.220.101.47

Domain: update-service[.]xyz

Hash (SHA256): 3a7f2c9b1d4e6f8a...

User-Agent: Mozilla/5.0 (compatible; MSIE 9.0)

行為: 深夜 02:00-04:00 大量 DNS 查詢，目標為金融業 SWIFT 系統

S – Style / Format

輸出使用結構化報告格式，包含：執行摘要 (3句以內)、IoC 對應 ATT&CK 技術編號、歸因信心度 (請

E – Evaluation

成功標準：每個 IoC 均對應至少一個 ATT&CK 技術 ID (T1xxx)，歸因需引用可驗證的公開情資 (如



- Result :

**** 1 執行摘要****

- 185.220.101.47 與域名 *update-service.xyz* 在 02:00-04:00 之間對金融機構 SWIFT 系
- 此行為對應 MITRE ATT&CK 的「DNS 偵查」與「遠程系統偵測」技術，屬於已知的金融機構 APT
- 建議立即阻斷相關網域/IP，部署高頻 DNS 監控規則，並在端點防護平台封鎖對應哈希值。

2 IoC 對應 MITRE ATT&CK 技術

IoC	ATT&CK 技術	描述	參考資料
IP 185.220.101.47	T1049 - 系統網路連線偵測 / T1583.001 - 域名註冊	來源 IP	
Domain update-service.xyz	T1518.001 - DNS 偵查 / T1583.001 - 域名註冊	該	
Hash 3a7f2c9b1d4e6f8f...	T1204 - 社交工程 / T1064 - 腳本/程式碼	哈希值屬於已	
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0)	T1071.001 - Web 內部通訊 (H		
行為：深夜 02:00-04:00 大量 DNS 查詢，目標為金融業 SWIFT 系統 T1518.001 - DNS			

3 歸因信心度

目標	信心度	理由
FIN7 / FIN8	**高**	- 2024 年 FireEye 針對 FIN7 的最新報告將 *update-servi
其他 APT	低	無其他已知 APT 在 185.220.101.47 或 *update-service.xyz* 上發

4 即時行動建議 (Top 3)

#	建議	可執行步驟 / 工具
1	**封鎖 IP / 域名**	- 在防火牆/NGFW 內新增封鎖規則，阻止所有進出 185.220.101.47
2	**部署高頻 DNS 監控規則**	- 在 SIEM (如 Splunk, ELK, QRadar) 建立規則：
3	**封鎖哈希及加強端點防護**	- 在 EDR/AV (CrowdStrike, SentinelOne, Microsoft

****備註****

- 建議在 30 分鐘內完成封鎖與規則部署，以減少後續攻擊窗口。
- 若已知 SWIFT 系統使用內部 DNS 伺服器，請在該伺服器上設置白名單僅允許可信域名。
- 追蹤後續事件：若仍出現相同哈希或域名的疑似活動，請考慮升級至全網絡級別的封鎖 (如 Cloudf



- One-Shot Prompt

角色設定

你是一名威脅情資分析師，專責將原始 IoC 轉化為可行動的情資報告 (Actionable Intelligence)

【示範範例 – 輸入】

IP: 45.142.212.100

Domain: cdn-support[.]net

行為: PowerShell 執行 Encoded Command，目標為 LSASS 記憶體傾印

【示範範例 – 期望輸出】

▶ 執行摘要

偵測到憑證竊取行為，IP 已見於 Cobalt Strike C2 基礎設施，歸因信心度：中。

▶ ATT&CK 對應

T1059.001 (PowerShell) · T1003.001 (LSASS Memory Dump) · T1071.001 (C2 over HTTP)

▶ 歸因

與 FIN7 / Carbanak 使用的 PS 混淆手法高度重疊 (信心度：中，依據：VirusTotal Passive DI)

▶ 即時行動 (Top 3)

1. 立即封鎖 45.142.212.100 於邊界防火牆
2. 部署 SIGMA 規則偵測 PowerShell -EncodedCommand 執行
3. 稽核所有 LSASS 存取事件 (Event ID 10 + Sysmon)

【現在請分析此新 IoC】

IP: 91.108.56.200

Domain: telegram-cdn[.]io

行為: 使用 Telegram Bot API 作為 C2 通道，每 5 分鐘 beacon，受害者為台灣政府機構



- Result :

▶ ****執行摘要****

偵測到利用 ****Telegram Bot API**** 作為 C2 通道，機器人每 5 分鐘 beacon 以取得指令。目標

▶ ****ATT&CK 對應****

- ****T1071.004**** (Web Services - Telegram Bot API)
- ****T1053.005**** (Scheduled Task/Job - 5-分鐘 beacon 節奏)
- ****T1105**** (Ingress Tool Transfer - 若後續使用 Telegram 下載 payload)

▶ ****歸因****

與 ****APT33**** (已於 2024 年透過 Telegram Bot API 與北韓間諜組織聯手執行指令) 以及 ****APT1**** 信心度：中等。根據 ****OpenCTI**** 與 ****Mandiant 2024**** 報告中列出的 Telegram C2 例證與相

▶ ****即時行動 (Top 3) ****

1. ****封鎖 IP / DNS****

- 在邊界防火牆及內部網路上即時封鎖 91.108.56.200 與域名 telegram-cdn.io。
- 配置 DNS 反向代理，攔截所有發往 telegram-cdn.io 的 HTTPS 請求。

2. ****偵測與告警****

- 部署 IDS/IPS 規則 (e.g., Suricata/Snort) 偵測對 ****https://api.telegram.org/****
- 在 SIEM 中加入 ****Sigma**** 規則，檢測 ****HTTP/HTTPS**** 連線至 Telegram Bot 域名，並

3. ****環境加固與排除****

- 檢查所有台灣政府機構內部伺服器，排查已安裝或正在執行的 Telegram Bot 客戶端程序。
- 實施 ****Web Application Firewall (WAF)**** 以阻擋不明 Bot Token，並將 ****HTTPS****
- 若發現有機器人程序，立即停止其服務並進行惡意程式分析，確認是否為後門或 C2 代理。

****備註****：若後續有新資訊顯示該 Bot 下載或執行 payload，請再追加 T1105 及相關的持續性技術



- Few-Shot Prompt

角色設定

你是一名威脅情資分析師。以下提供 3 個不同攻擊向量的分析範例，學習其推理模式後，對第 4 個新

範例 1 – 勒索軟體初期滲透

向量：惡意 Office 巨集 → VBA 執行 mshta.exe → 下載 Cobalt Strike beacon

域名：office365-update[.]top

情境分類：初始存取 (Initial Access)

ATT&CK：T1566.001 · T1059.005 · T1218.005

歸因信心：中 – 與 LockBit 3.0 附屬組織手法重疊

行動：停用 Office 巨集 (GPO) · 封鎖 mshta.exe 外連 · 部署 EDR 偵測規則

範例 2 – 供應鏈攻擊

向量：受污染的 npm 套件 → 後門植入 → 竊取 CI/CD 環境變數與 AWS 金鑰

套件名：node-fetch-extra@2.1.4 (偽冒合法套件)

情境分類：供應鏈入侵 (Supply Chain Compromise)

ATT&CK：T1195.001 · T1552.001 · T1078.004

歸因信心：低 – 手法泛用，難以特定歸因至已知組織

行動：稽核 package-lock.json · 輪換所有受暴露金鑰 · 啟用 npm audit 於 pipeline

範例 3 – APT 橫向移動

向量：DCSync 攻擊竊取 AD 雜湊值 → Pass-the-Hash → 存取財務伺服器

行為觸發時間：工作日 03:15，來源帳號為已離職員工

情境分類：憑證存取 + 橫向移動 (Credential Access + Lateral Movement)

ATT&CK：T1003.006 (DCSync) · T1550.002 (Pass-the-Hash) · T1078.002

歸因信心：高 – 手法與 APT41 報告高度吻合 (信心依據：CrowdStrike 2024 IR 報告)

行動：立即停用離職帳號 · 重置 krbtgt 密碼兩次 · 稽核 AD Replication 權限

【請分析此新案例 (第 4 案)】

向量：攻擊者使用 Living-off-the-Land 手法，透過 certutil.exe 下載惡意 DLL

→ DLL Side-Loading 注入至 svchost.exe

→ 建立排程工作 (Scheduled Task) 確保持久性

→ 使用 DNS over HTTPS (DoH) 規避傳統 DNS 監控

目標產業：台灣半導體製造業

時間特徵：僅在台灣工作日 08:00-17:00 活躍

請輸出：情境分類 · ATT&CK 技術 ID (含子技術) · 歸因信心度與依據 · 即時行動建議 Top 3 · 畧

- Result :

****情境分類****

- Persistence + Command & Control

****ATT&CK 技術 ID (含子技術) ****

- T1105 - Ingress Tool Transfer (certutil.exe)
- T1129 - DLL Side-Loading (svchost.exe)
- T1053.005 - Scheduled Task/Job (persistence)
- T1071.004 - Application Layer Protocol: DNS (DoH)
- T1059.003 - Windows Command Shell (certutil execution)

****歸因信心****

- ****中**** -
 - 這些技術組合 (Living-off-the-Land certutil → DLL side-loading → DoH → schedule)
 - 目標為台灣半導體製造業且僅於工作時間內活躍，符合 APT41 近期針對台灣/亞太半導體業者的特徵
 - 然而，certutil、DLL side-loading 與 DoH 皆為多個 APT (APT41、APT30、Lazarus 等) 的技術

****即時行動建議 (Top 3) ****

1. ****阻止 & 監控 certutil.exe****
 - 在所有受影響主機上即時將 certutil.exe 標記為禁止執行或使用 AppLocker/Defender Application Control
2. ****審查 & 停用可疑 Scheduled Task****
 - 搜尋 Windows 事件日誌 (事件 ID 4698/4699) 與 Task Scheduler，列出所有於工作時間內執行之 Task
3. ****強制 DLL 簽名 & 限制 svchost.exe****
 - 使用 Windows Defender Application Control / AppLocker，設定 svchost.exe 僅允許執行已簽名之 DLL

****額外情資收集建議****

- ****certutil 執行分析****
 - 捕捉 certutil.exe 的完整命令列與下載 URL，對照已知惡意域名/IP。
- ****下載 DLL 深層分析****
 - 在沙盒中執行、YARA 搜尋、AV 掃描，確認是否屬於已報告的 APT41 工具集或其他已知威脅。
- ****DoH 連線追蹤****
 - 監控 DNS over HTTPS 請求，記錄目標域名、IP 與時序；對照威脅情報 (C2、Command-and-C&C)
- ****事件時間相關檢索****
 - 針對 08:00-17:00 的活動窗口，對照事件日誌、網路流量與可疑任務創建時間，辨識是否為有意攻擊
- ****產業特定情報****
 - 收集台灣半導體製造業最近的攻擊報告 (APT41、APT30 等)，比對腳本、C2 域與行為模式。

透過上述即時防禦與深入情報蒐集，可在最短時間內阻斷持續性威脅，並為後續鑑定與追蹤提供足夠證據。



- Prompt Template :

Additional Context

- Suspected Actor: {{apt_group}}
- Known Campaign: {{campaign}}
- Malware Family: {{malware}}

Enhanced Tasks

1. Attribution Analysis

- Match TTP similarity with known APT groups
- Infrastructure overlap
- Historical patterns

2. Campaign Modeling

- Timeline reconstruction
- Targeting pattern

3. Strategic Intent

- Espionage / Financial / Disruption

4. Kill Chain Mapping

- Reconnaissance → Weaponization → Delivery → Exploitation → C2 → Actions

新增對話

搜尋

筆記

工作區

對話

今天

Taiwan Semiconductor APT Alert

Telegram Bot C2 Target

Fin7 SWIFT Threat Analysis

Anxun Threat Intelligence

Anxun Threat Detection

成都404 指紋

模型 知識 **提示詞** 工具

threat intelligence analysis

/threat-intelligence-analysis

提示詞內容

Additional Context

- Suspected Actor: {{apt_group}}
- Known Campaign: {{campaign}}
- Malware Family: {{malware}}

Enhanced Tasks

1. Attribution Analysis
 - Match TTP similarity with known APT groups
 - Infrastructure overlap
 - Historical patterns
2. Campaign Modeling
 - Timeline reconstruction
 - Targeting pattern
3. Strategic Intent
 - Espionage / Financial / Disruption
4. Kill Chain Mapping
 - Reconnaissance → Weaponization → Delivery → Exploitation → C2 → Actions

ⓘ 使用方括號格式化您的變數，如下所示：{{變數}}。請務必將它們放在 {{ 和 }}。
[To learn more about powerful prompt variables, click here](#)

/threat-intelligence-analysis
 threat intelligence analysis

ⓘ 提示：在每次替換後按下對話輸入框中的 Tab 鍵，即可連續更新多個變數欄位。

/

+ 程式碼直譯器

🎤 ⬆

Open WebUI - v0.6.18

Input Variables



apt_group *required

APT41

campaign *required

APT41

malware *required

Winnti

取消

儲存


Additional Context

- Suspected Actor: APT41
- Known Campaign: APT41
- Malware Family: Winnti

Enhanced Tasks

1. Attribution Analysis

- Match TTP similarity with known APT groups
- Infrastructure overlap

+  程式碼直譯器



- Result :

Attribution Analysis - APT41 (Winnti)

#	Focus	Findings	Key Indicators
1	TTP Similarity	APT41's use of Winnti malware is almost identical to e	
2	Infrastructure Overlap	Over the last 8 years, the same DNS zones, hos	
		• Domains - *.winnti.cn, *.h5mail.cn, *.zxx.com, *.xiaohei.com.<	
3	Historical Patterns		
		• Early Years (2015-2017) - Targeted game developers, military vendors,	

Attribution Verdict

The convergence of **TTPs, infrastructure, and timeline** strongly supports the a

Campaign Modeling

1. Timeline Reconstruction

Date/Period	Event	Technical Detail	Impact
2015-06	First public Winnti release	DLL injector (Winnti.dll)	Initi
2016-11	Supply-chain attack on Kaspersky	Custom DLL inside Kaspersky ir	
2017-02	Exchange vulnerability exploitation (CVE-2017-11882)	Remote coc	
2018-08	Winnti-Stealer in China	Stole credentials for webmail, banking,	
2019-10	0-day CVE-2019-0708 ("BlueKeep") usage	RDP exploitation + Winnt	
2020-03	CVE-2021-26855 (Exchange) exploitation	RCE + Winnti persistence	
2021-05	0-day CVE-2021-31166 exploitation	Windows "Winlogon" injection	
2022-12	Targeted banking sector in Southeast Asia	Phishing + Winnti + c	
2023-07	Latest Winnti version "Winnti-5"	Cloud-native C2, TLS-encrypted	

> **Key Milestone** - The **2021-05** CVE-2021-31166 incident marked the shift fr

2. Targeting Pattern

Sector	Frequency	Typical Entry Point	Observed Malware
Gaming	High (40 %)	Social engineering + malicious DLLs	Winnti-Stealer
Defense/Defense-Contractors	Medium (25 %)	Phishing + supply-chain	Wir
Financial/Banking	Medium (20 %)	Credential harvesting + RDP	Winnti +
Healthcare	Low (10 %)	Zero-day exploitation (CVE-2021-26855)	Winnti
Public Sector	Low (5 %)	Exploit public servers	Winnti

Pattern: APT41 consistently exploits **vulnerabilities** in widely deployed softv

Strategic Intent

Intent	Evidence	Likely Motivation
Espionage	• Targeted defense contractors	• Stolen credentials from mi
Financial	• Crypto-mining module in Winnti-5	• Exfiltration of bankir
Disruption / Sabotage	• Use of zero-day CVEs to cripple infrastructure	
Hybrid	• Combination of all three above in single campaigns	Flexibil

> **Primary Focus:** **Espionage** is the overarching goal, with **financial expl**

Kill Chain Mapping (APT41 - Winnti)

Kill-Chain Stage	APT41 TTP	Winnti-specific Detail	Example Artifacts
Reconnaissance	• OSINT (LinkedIn, Twitter)	• Passive domain registrati	
Weaponization	• Custom DLL (`Winnti.dll`)	• PowerShell scripts	• DLL
Delivery	• Phishing emails	• Drive-by downloads	• Attachments `invoi
Exploitation	• CVE-2021-26855 (Exchange)	• RDP exploitation (CVE-2019-	
Installation	• Persistence via registry run key	• `HKCU\Software\Micros	
Command & Control (C2)	• HTTP/HTTPS over TLS	• Encrypted payload delive	
Actions on Objectives	• Credential theft (webmail, banking)	• Data ext	
Exfiltration	• Lateral data transfer	• Chunked TLS uploads to C2	`POS
Impact	• Disruption of gaming services	• Theft of intellectual propert	

> **Key Observations**

> * The **C2** channel evolves from plain HTTP to **TLS-encrypted HTTPS** with cu

> * The **weaponization** layer uses **DLL injection** to hide within legitimate

> * **Exploit chain** often starts with a public vulnerability (CVE) to gain an i

Recommendations

- Threat Hunting** - Focus on:
 - * Unexpected DLL loads into `winlogon.exe`, `steam.exe`, or `w3wp.exe`.
 - * Registry Run key entries with "Winnti" or "winnti.dll" names.
 - * Outbound HTTPS traffic to suspicious domains (`*.winnti.cn`, `*.h5mail.cn`).
- Patch Management** - Prioritize:
 - * CVE-2021-26855 (Exchange), CVE-2019-0708 (RDP), and CVE-2021-31166.
 - * End-of-life Windows systems; consider moving to managed services.
- Endpoint Detection & Response (EDR)** - Deploy sensors capable of:
 - * Detecting **DLL injection** patterns.
 - * Monitoring for **cryptocurrency mining** processes (high CPU usage, `winnti-

4. **Network Segmentation** - Restrict RDP and SMB access to internal hosts only;

5. **Incident Response Playbook** - Include steps for:

- * Isolating infected hosts with `winnti.dll`.
- * Performing a forensic memory dump to confirm malicious processes.
- * Rolling back registry changes and removing malicious DLLs.

Bottom Line

APT41 continues to rely on the **Winnti malware family** to achieve a blend of **malicious**

TASK 2: Advanced Chat Control Usage

<https://api-dashboard.search.brave.com/app/keys> (<https://api-dashboard.search.brave.com/app/keys>).

Add new API key



You may have up to 10 keys per subscription (i.e., 10 for Search, 10 for Spellcheck, etc.). Distinct keys help to distinguish between development and production environments.

Name *

Subscription *

Cancel



API keys

Go to the [Available plans](#) page to subscribe to a plan before generating API keys. You may have up to 10 keys per plan.

Search

[+ Add API key](#)

Your API keys for this plan.

NAME	API KEY			
30cm	BSAP.....			Remove

🔔 This plan supports 50 requests per second and unlimited requests per month total. You can generate multiple keys, but all requests count toward this shared limit.

The screenshot shows the settings for the '網頁搜尋' (Web Search) feature. The '設定' (Settings) tab is active. The 'Brave 搜尋 API 金鑰' (Brave Search API Key) is set to 'BSAPIMyNqheSBzrdibhiuoj9UHOHIONY'. The '搜尋結果數量' (Search Results Count) is set to 3. The 'admin' user is logged in.

- Prompt : 全台灣最頂的資安研究所是哪間？
- No web search :

在台灣，若從「資安研究實力、國際知名度、人才培養與產學合作」等面向綜合評估，**國立台灣大學

為何 NTU 被視為台灣資安研究的頂尖機構？

項目	具體情況	主要貢獻
研究實力	NTU 資安實驗室擁有國際級的研究團隊，涵蓋	**資訊安全、隱私保護、漏洞分析
人才培養	毕业生多數進入台灣政府機關、國防部、半導體、金融、電信等關鍵產業，亦有不	
產學合作	與多家企業（如華為、聯發科、台積電、台灣電力、行政院網路安全辦公室）合作	
國際合作	與美國加州大學伯克利分校、麻省理工學院、香港科技大學等機構共建研究中心。	
資源與基礎設施	擁有大型網路安全實驗室、模擬攻擊平台（CTF、沙盒）和大型計算資源。	

其他值得關注的台灣資安研究單位

機構	特色
國立陽明交通大學（NYCU）資訊安全研究中心	以「資訊安全與隱私」為核心，強調雲端安全
國立中央大學資訊安全研究中心	在行動安全、智慧城市安全等方面有突出貢獻。
中研院資訊科學研究所	以理論基礎研究為主，研究方向包括「密碼學、信息理論安全」等。
台灣電力公司（TAEC）網路安全中心	與 NTU 合作，實務導向研究，重點在關鍵基礎建設安

小結

- **國立台灣大學（NTU）** 的資安研究機構，無論是學術影響力、人才培育、產學合作還是國際合作，都在台灣處於領先地位，被廣泛認為是「全台最頂尖的資安研究所」。
- 其他學術機構如 NYCU、國立中央大學也有突出的資安研究，但相較於 NTU 的整體影響力與資源規模，略遜一籌。

如果你有進一步的需求（如想參加研究、申請獎學金或合作），可直接聯繫 NTU 資安實驗室的研究團隊，他們會提供更具體的協助。祝你在資安領域取得佳績！



• web search :

全台灣最頂尖的資訊安全（資安）研究所通常被認為是**國立臺灣大學（NTU）**的資安研究中心／電機系資訊安全碩士班，因為其在學術研究、產業合作以及人才培育方面均居領先地位[2][7]。其他在資安領域同樣具備強大研究實力的學府還包括國立清華大學、國立中山大學等，但在整體評比與國際影響力上，臺大往往被列為首選。



Explanation of the mechanism and reflection

Open WebUI Web Search Tool 運作原理

Open WebUI 的網路搜尋功能本質上是一套 **Web Search RAG (Retrieval-Augmented Generation)** 管線，它並非讓模型直接「上網」，而是透過後端代理搜尋、擷取、清理並注入外部資訊至模型上下文，再由模型生成回覆。

整體資料流架構

當使用者在對話框啟用網路搜尋並送出問題，Open WebUI 會依序執行以下流程：

1. **觸發查詢**：使用者問題送往後端，判斷需要即時資訊
2. **呼叫搜尋引擎 API**：透過 `backend/open_webui/retrieval/web/main.py` 中的 `search_web()` 函數，依設定呼叫對應引擎 (Google PSE、Brave、SearXNG 等)
3. **爬取並清理內容**：對搜尋結果前 N 筆 (由 `RAG_WEB_SEARCH_RESULT_COUNT` 控制) 進行 HTML 抓取，轉換為 Markdown 或純文字
4. **Context Injection (上下文注入)**：清理後的文字透過 RAG Template 注入至模型的 system prompt 或 user message 前綴
5. **模型推理生成回覆**：LLM 在獲得外部資訊的脈絡下生成更即時、準確的答案

與傳統 RAG 的差異

傳統 RAG 仰賴靜態向量資料庫 (如 ChromaDB、Milvus) 進行語意相似度檢索，而 Web Search RAG 屬於**動態即時版本**：

面向	傳統文件 RAG	Web Search RAG
資料來源	本地向量資料庫	即時網路搜尋結果
分塊/Embedding	預先建立索引	無，直接注入原始文字
時效性	依上傳時間	即時
延遲	低 (本地查詢)	高 (網路 I/O + 重新 tokenize)
Context 污染風險	低	高 (HTML 雜訊、廣告)