政府機關資安威脅與防護重點

簡報人員：張慧宇經理
簡報單位：威脅分析中心

大綱

- 全球資通安全威脅趨勢
- 政府資通安全威脅趨勢
- 政府資安事件案例分析
- 政府機關資安防護強化重點
- 結論與建議

國家資通安全研究院
National Institute of Cyber Security

全球資通安全威脅趨勢

全球資通安全威脅趨勢

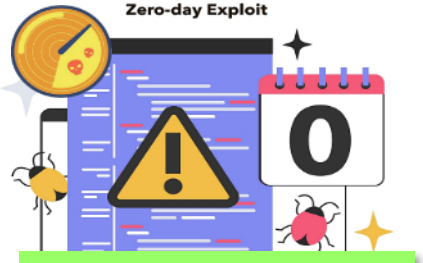
- 綜整114年上半年全球資安威脅情資，由網際攻擊狙殺鍊(Cyber Kill Chain)歸納資安威脅趨勢，可分為六大類

偵查、武裝、遞送

攻擊、安裝

PII 與憑證外洩導致保護機制失效

雲端應用服務衍生多元威脅



資通系統弱點頻遭揭露利用

社交工程泛濫致APT鎖定與勒索軟體風險增加

資安(訊)供應鏈遭駭破壞邊界信任與防護

駭客利用AI技術開發新型攻擊與惡意詐欺

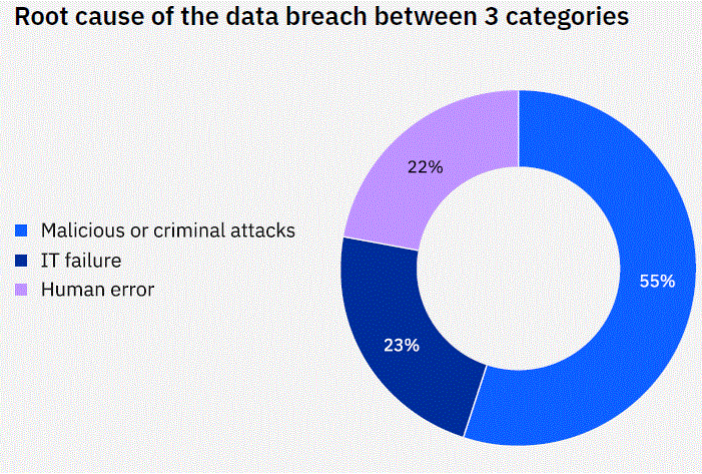
發令與控制

採取行動

PII 與憑證外洩導致保護機制失效

- 資安廠商 Verizon 2025 資料外洩報告(Data Breach Investigations Report)
  - 主要資料外洩案件皆涉及人為因素，占6成之多，社交工程與憑證濫用有顯著關聯性
  - 次之有30%資料外洩事件與第三方有關(包含軟體漏洞)，主要集中在針對邊界設備與 VPN 的零日漏洞攻擊
  - 第三名為間諜活動驅動之入侵事件顯著成長，已達到17%
- 個資外洩案例：
  - 美國總統川普國安顧問使用通訊軟體Signal討論即將發動的葉門軍事行動引起軒然大波，部分高層官員的聯絡資料，包括手機號碼，可於網路上查詢
  - DeepSeek 發生重大資料洩露，洩露逾百萬筆敏感記錄，洩漏之資訊包含聊天記錄、後端詳細資訊、API 及操作資訊等

資料外洩主因



來源: https://www.ibm.com/reports/data-breach

雲端應用服務衍生多元威脅

- 雲端應用趨勢成長驚人，Gartner預測到 2027 年，90% 的組織將採用混合雲，2025年所有雲端運算領域都將達到兩位數成長，全球終端用戶在公有雲服務上的支出預計將從 2024 年的 5,957 億美元成長到 2025 年的 7,234 億美元
- 雲端安全聯盟(CSA)於雲端運算面臨的主要威脅深度剖析報告(Top Threats to Cloud Computing Deep Dive 2025)，指出雲端資安事件中最常見的安全威脅如下
  - IAM – 存取控制薄弱、缺乏多因子鑑別(MFA) 以及權限提升導致未經授權的存取
  - 配置錯誤和變更控制不足－雲端環境安全措施不當導致資料長期暴露
  - 軟體開發不安全－軟體開發、交付及部署實務薄弱，導致安全漏洞
- 雲端服務遭攻擊案例：美國網路安全暨基礎設施安全局(CISA)4月時發布與潛在舊版 Oracle 雲端入侵相關的憑證風險指南，緣由為CloudSEK 發布一份報告，聲稱駭客竊取了Oracle Cloud超過 600 萬筆記錄，影響逾 14 萬名租戶

來源:paloalto雲端原生安全現狀報告,最受關切的雲端安全問題

資通系統弱點頻遭揭露利用

- 資安廠商 ReversingLabs 2025軟體供應鏈安全報告(Software Supply Chain Security Report)
  - 一項針對 30 個 npm、PyPI 和 RubyGems 套件之調查發現，開源軟體包的最新版本中潛伏著大量嚴重且可利用的漏洞，這些軟體包在這 30 個軟體包與3個軟體包管理器中
  - 總下載量超過 6.5 億次，每個軟體包發現的安全漏洞中位數為 27 個(平均 68 個)，其中每個軟體套件有 2 個嚴重漏洞(平均 6 個)
  - 113年 npm 機密洩露的主要來源，Google 、 AWS 、GitHub 、Slack 、npm 、Discord 、Telegram、OpenAI、Azure
- 個資外洩案例：
  - CISA 將一個嚴重的 9.8 Langflow 漏洞新增至已知被利用漏洞 (KEV) 目錄中，Langflow 在開發人員愛用之GitHub 上擁有近 60,000 名用戶，其未經身份驗證的 RCE 漏洞可讓攻擊者在沒有憑證或用戶允許情況下完全控制伺服器
  - Cisco Webex App高嚴重性漏洞，可讓駭客透過會議連結取得程式碼執行權限

2025 年十大易被利用漏洞

List of Top 10 Exploited Vulnerabilities

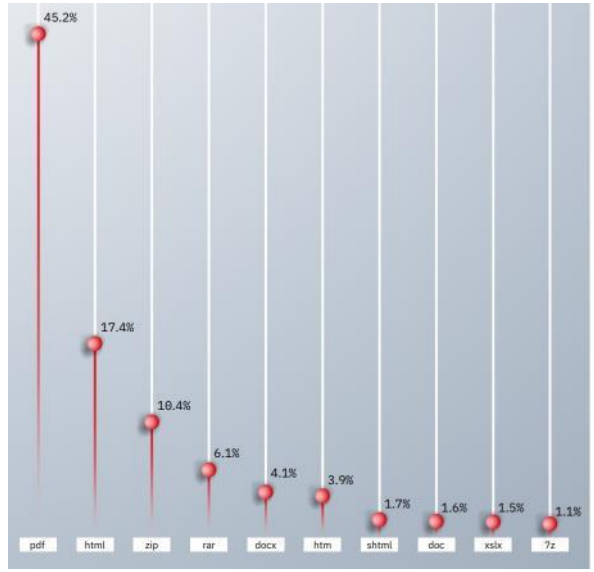
1. ZeroLogon (CVE-2020-1472)
2. Log4Shell (CVE-2021-44228)
3. ICMAD (CVE-2022-22536)
4. ProxyLogon (CVE-2021-26855)
5. Spring4Shell (CVE-2022-22965)
6. Atlassian Confluence RCE (CVE-2022-26134)
7. VMware vSphere (CVE-2021-21972)
8. Google Chrome Zero-Day (CVE-2022-0609)
9. Follina (CVE-2022-30190)
10. PetitPotam (CVE-2021-36942)

來源: https://www.getastra.com/blog/security-audit/top-vulnerabilities/

社交工程泛濫致APT鎖定與勒索軟體風險增加

- 資安廠商IBM於2025威脅情報指數(X-Force 2025 Threat Intelligence Index)，指出
  - 每週透過網路釣魚郵件傳播的資訊竊取程式數量增加 84%。X-Force 發現，透過網路釣魚郵件與憑證網路釣魚傳播的資訊竊取程式數量逐年增加
  - 駭客運用AI建立網站，並於網路釣魚攻擊中加入深偽技術，建立網路釣魚電子郵件且編寫惡意程式碼
  - 勒索軟體在 2024 年惡意軟體案件中占比最高，達到 28%
- 社交工程攻擊案例：
  - Darcula 網路釣魚即服務已導致 80 萬多名受害者，誘騙受害者點擊冒充快遞公司等品牌的 SMS、RCS 及iMessage 文字。受害者被要求支付運費才能收到他們的包裹或要求支付道路通行費等等
  - CoGUI 網路釣魚套件鎖定日本發送數百萬條社交工程訊息，冒充知名公司，如消費與金融品牌，主要竊取使用者名稱、密碼及付款資料

PDF 是排名第一的惡意附件檔案類型

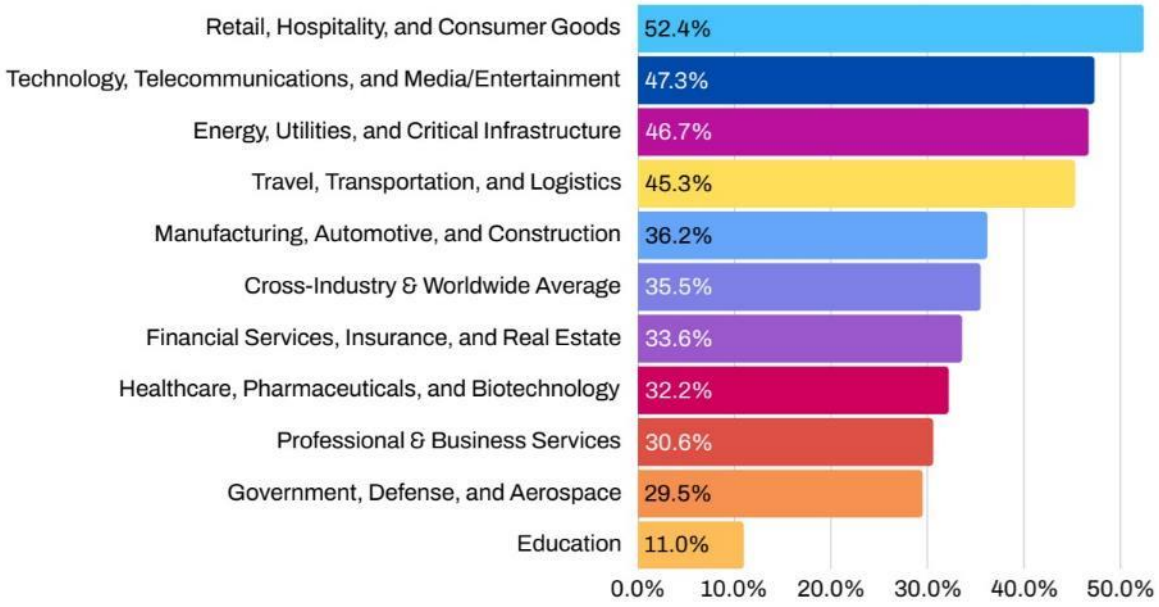


來源: https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index

資安(訊)供應鏈遭駭破壞邊界信任與防護

- 資安廠商 2025全球第三方資安事故報告(Security Scorecard Global Third-Party Breach Report)指出
  - 第三方資料外洩事件快速上升，35.5% 的資料外洩事件與第三方有關，高於去年的 29%
  - 攻擊者越來越多地利用第三方存取權限來規避強大的內部安全措施，主要攻擊來源為外包、夥伴關係及雲端利用
  - 第四方違規行為造成連鎖反應，涉及供應鏈中的另一個組織：第四方違規行為占所有違規行為的 4.5%，占第三方違規行為的 12.7%
- 供應鏈遭駭案例：
  - CrazyHunter勒索軟體攻擊台灣醫院
  - Hertz供應鏈攻擊，俄羅斯勒索團體Clop先攻擊Hertz的檔案管理服務提供商Cleo Communications零日漏洞，間接獲取Hertz的客戶資料，攻擊導致Hertz股票下跌2.5%，並對公司聲譽與客戶信任造成長期影響

因第三方違規行為致遭受影響之行業別排名

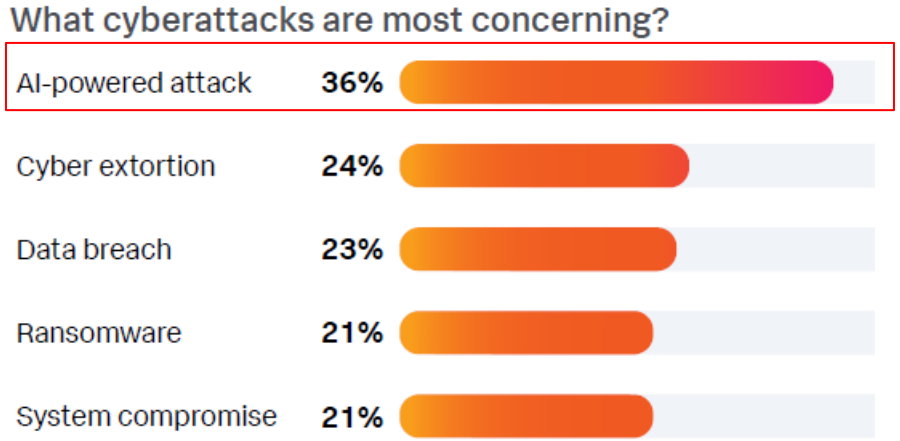


來源: https://securityscorecard.com/thank-you/content, 2025 SecurityScorecard Global Third-Party Breach Report

駭客利用AI技術開發新型攻擊與惡意詐欺

- PWC於2024全球數位信任洞察報告指出，生成式AI帶來的機會與風險同樣巨大：52%受訪企業認為在未來12個月，生成式AI可能導致災難性的網路攻擊
- 資料科學廠商Feedzai發表2025詐欺和金融犯罪預防中的人工智慧趨勢報告(AI Trends in Fraud and Financial Crime Prevention)，趨勢重點：
  - 92% 的受訪者表示，詐騙分子會使用生成式AI (GenAI)
  - 60%的受訪者認為犯罪分子正在利用生成式AI進行語音複製(Clone)詐騙
  - 44%的受訪者表示，深偽 (DeepFake) 被用於詐騙計劃
  - 56%的受訪者，社交工程被利用做為重要的AI入侵手段
  - 96%的金融機構使用生成式AI進行詐騙防治
- AI案例：惡意 AI 模型利用「Hugging Face」發展攻擊新手法，ReversingLabs 研究人員在 Hugging Face 平台發現惡意的機器學習(ML)模型，這些模型使用一種新穎的技術，透過濫用 Pickle 檔案序列化來散播惡意軟體。Hugging Face 做為一個流行的 AI 模型共享平台，已成為惡意行為者的目標，事件案例持續發生

最關注之網路安全議題



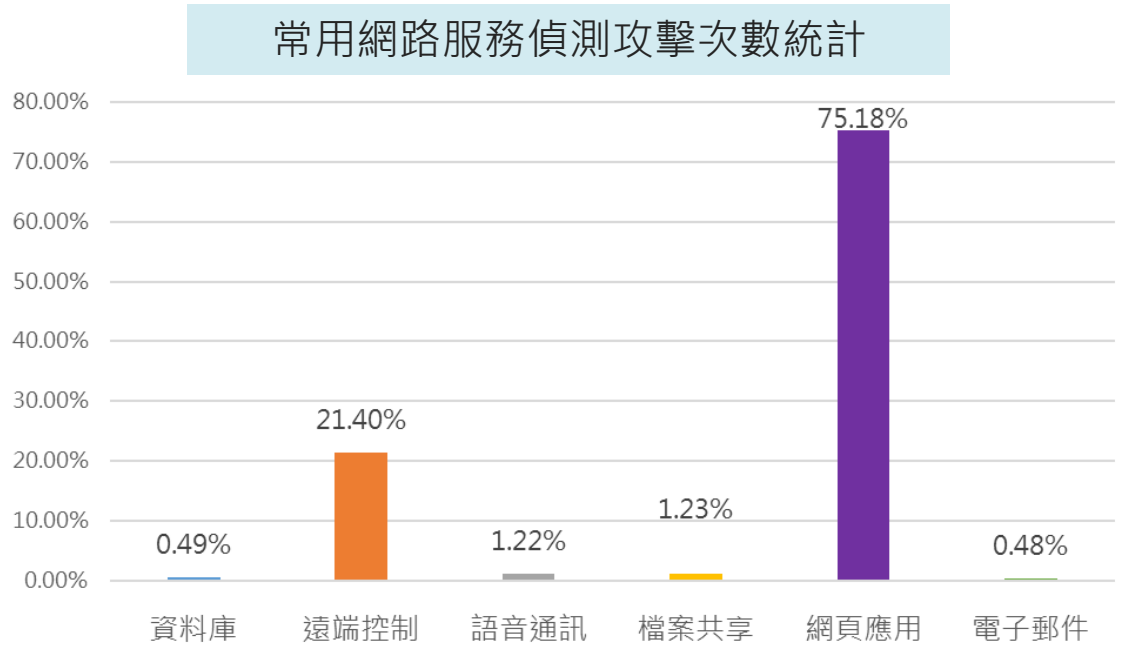
來源: State of Security, The Race to Harness AI, Splunk

國家資通安全研究院
National Institute of Cyber Security

政府資通安全威脅趨勢

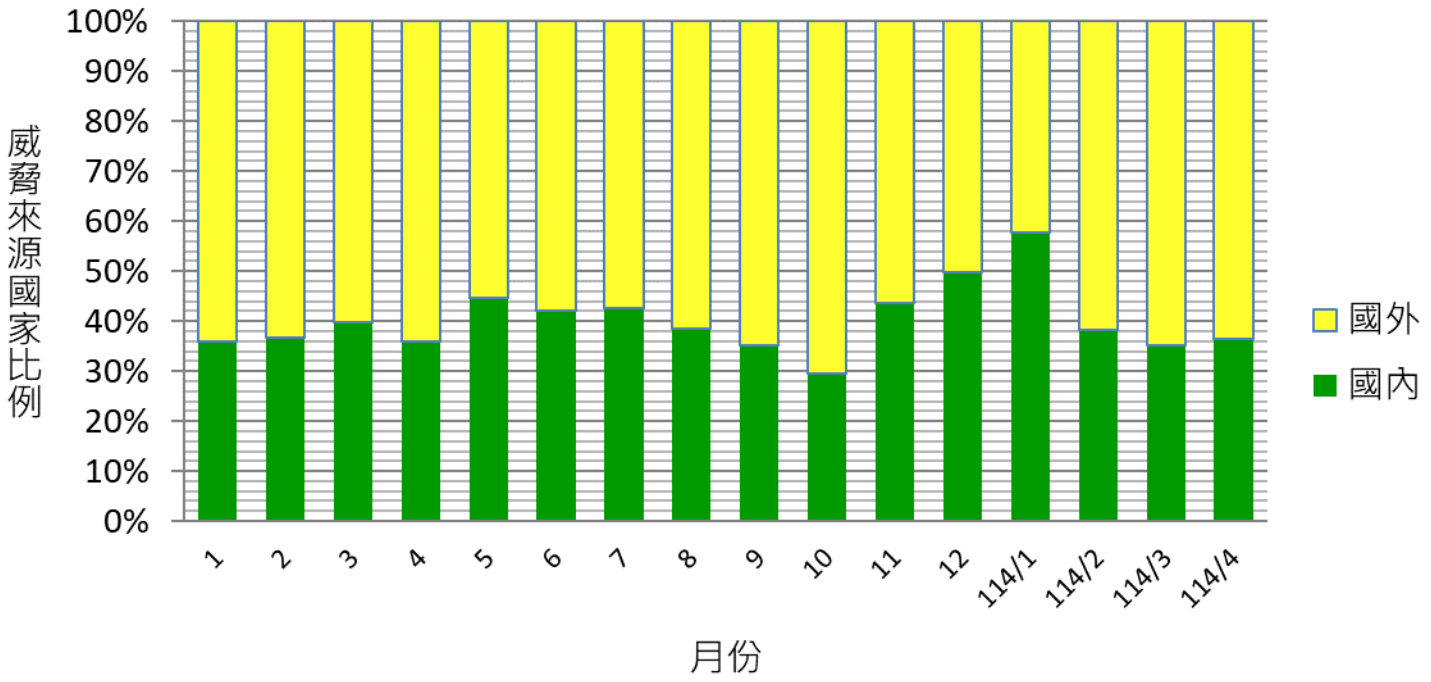
殭屍網路威脅情蒐

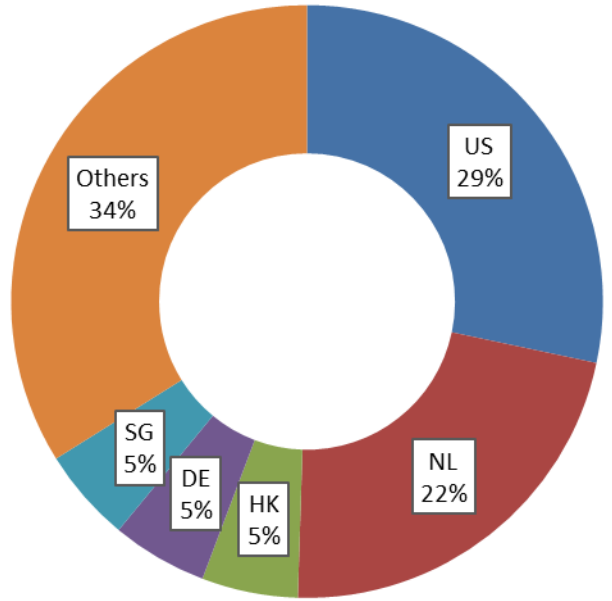
- 113年1月1日至114年4月30日透過國內外部署之蜜罐誘捕殭屍網路攻擊威脅
  - 前3名攻擊跳板來源國家分別為美國(31%)、保加利亞(12%)及俄羅斯(10%)
  - 常用網路服務受駭情形，以針對網頁應用服務之攻擊最為嚴重
  - 捕獲的惡意樣本中，以Mirai殭屍網路與其變種最多



聯防監控威脅情蒐(1/3)

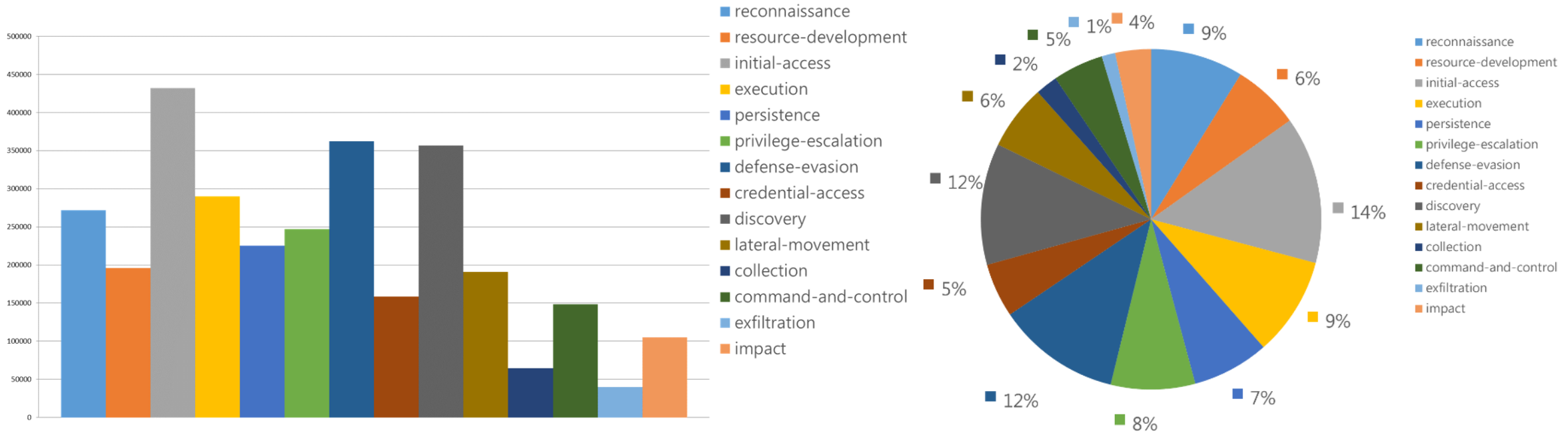
- 113年1月1日至114年4月30日，政府機關回傳有效資安監控情資依政府機關業務類別，前3名為綜合行政類之資訊蒐集類事件、外交國防法務類之資訊蒐集類事件、綜合行政類之入侵攻擊類事件
- 國外攻擊跳板來源前3名分別為美國(29%)、荷蘭(22%)及香港(5%)





聯防監控威脅情蒐(2/3)

- 統計MITRE ATT&CK框架之戰術（Tactic），其中，第1名為初始訪問（Initial Access）(14%)，主要是獲取系統的初始進入點，如釣魚攻擊或利用漏洞；其次為防禦規避（Defense Evasion）(12%)，大多為躲避安全機制，如禁用防毒軟體或混淆惡意程式碼；以及發現（Discovery）(12%)，主要是收集系統和網路資訊，如掃描開放端口或查詢使用者帳號



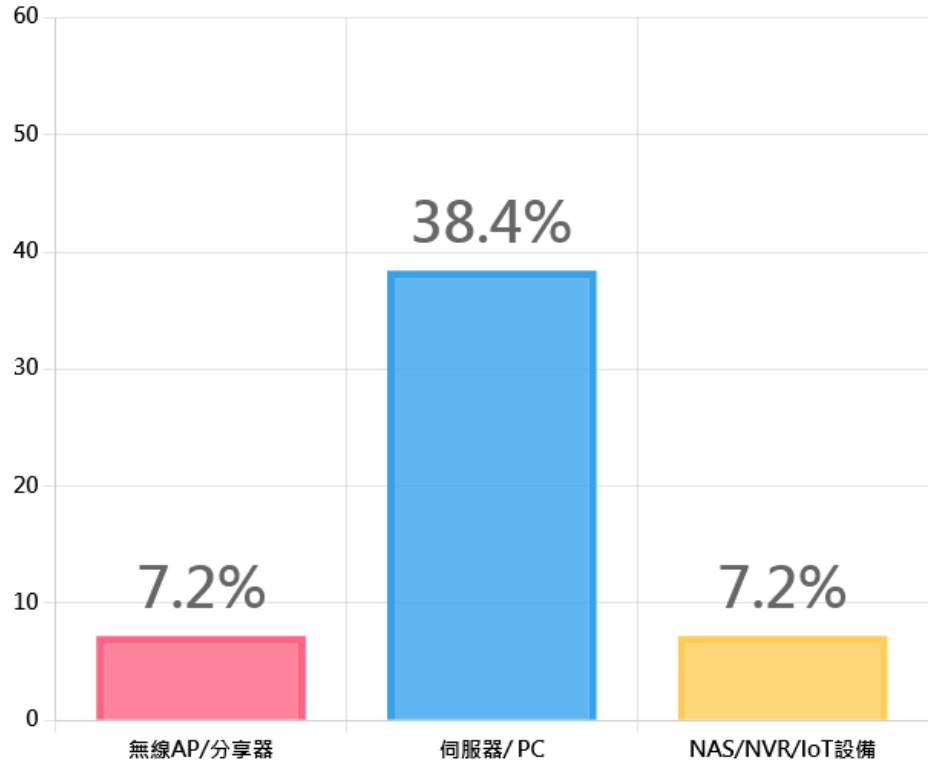
聯防監控威脅情蒐(3/3)

- 依業務類別統計，多數機關面臨之戰術前兩名多為攻擊中階段，包含Initial Access與Defense Evasion，主要技術(Technique)分別為Exploit Public-Facing Application與Impair Command History Logging
- 值得注意的是defense-evasion的手法各有不同，可強化偵測該階段

業務類別	Top2 戰術	主要攻擊手法
綜合行政	initial-access	Exploit Public-Facing Application
	discovery	Active Scanning
外交國防法務	discovery	Active Scanning
	initial-access	Exploit Public-Facing Application
經濟能源農業	initial-access	Exploit Public-Facing Application
	defense-evasion	SID-History Injection
內政衛福勞動	defense-evasion	Impair Command History Logging
	initial-access	Exploit Public-Facing Application
教育科學文化	defense-evasion	Impair Command History Logging
	execution	Visual Basic
非行政	initial-access	Exploit Public-Facing Application
	defense-evasion	SID-History Injection
財政主計金融	defense-evasion	Software Packing
	persistence	Kernel Modules and Extensions
交通環境資源	initial-access	Exploit Public-Facing Application
	impact	External Defacement

政府機關攻擊分析受駭裝置(1/2)

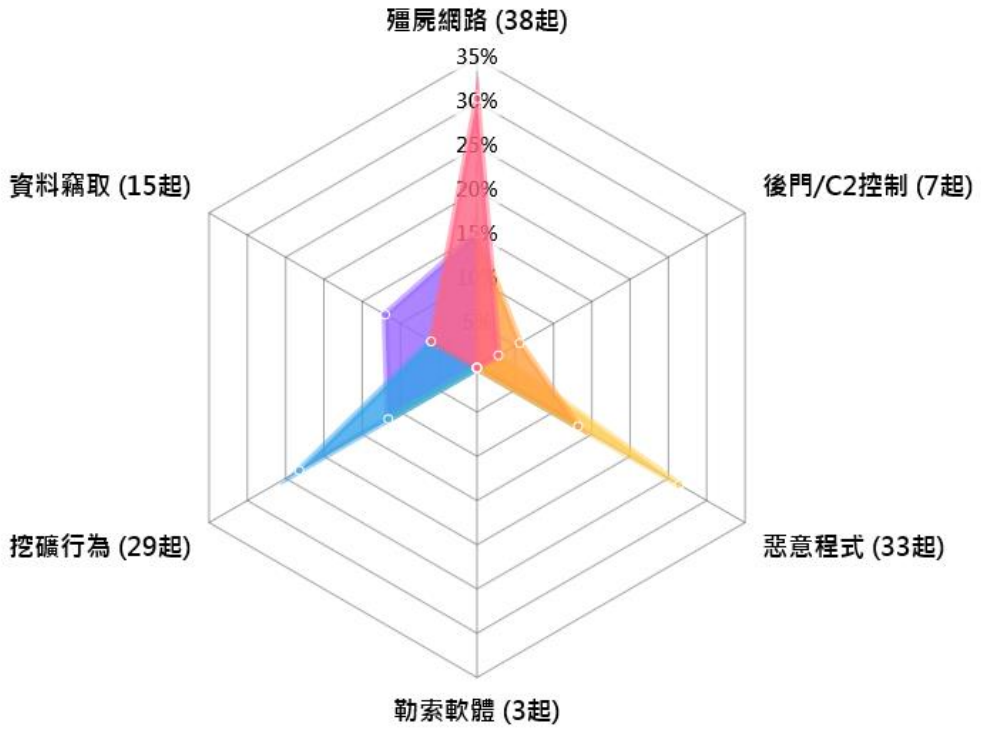
- 統計113年1月1日至114年4月30日政府機關攻擊分析發現並發布警訊通知之可識別受駭設備，以伺服器/PC受駭之比例為最多達38.4%，無限AP/分享器與NAS/NVR/IOT設備比例相同



- 無線AP/分享器
  - 因缺乏安全性更新導致容易成為攻擊目標
  - 以預設密碼或已知漏洞滲透後充當殭屍網路或跳板，隱匿攻擊來源
- 伺服器/PC
  - 具針對性目標的攻擊情境，可能具弱點漏洞或遭社交工程攻擊植入惡意程式
  - 取得內部資料或作為攻擊節點，用於橫向移動
- NAS/NVR/IoT設備
  - 針對嵌入式系統攻擊常利用弱密碼或老舊韌體植入惡意程式。更新管控與監測能見度低

政府機關攻擊分析受駭情形(2/2)

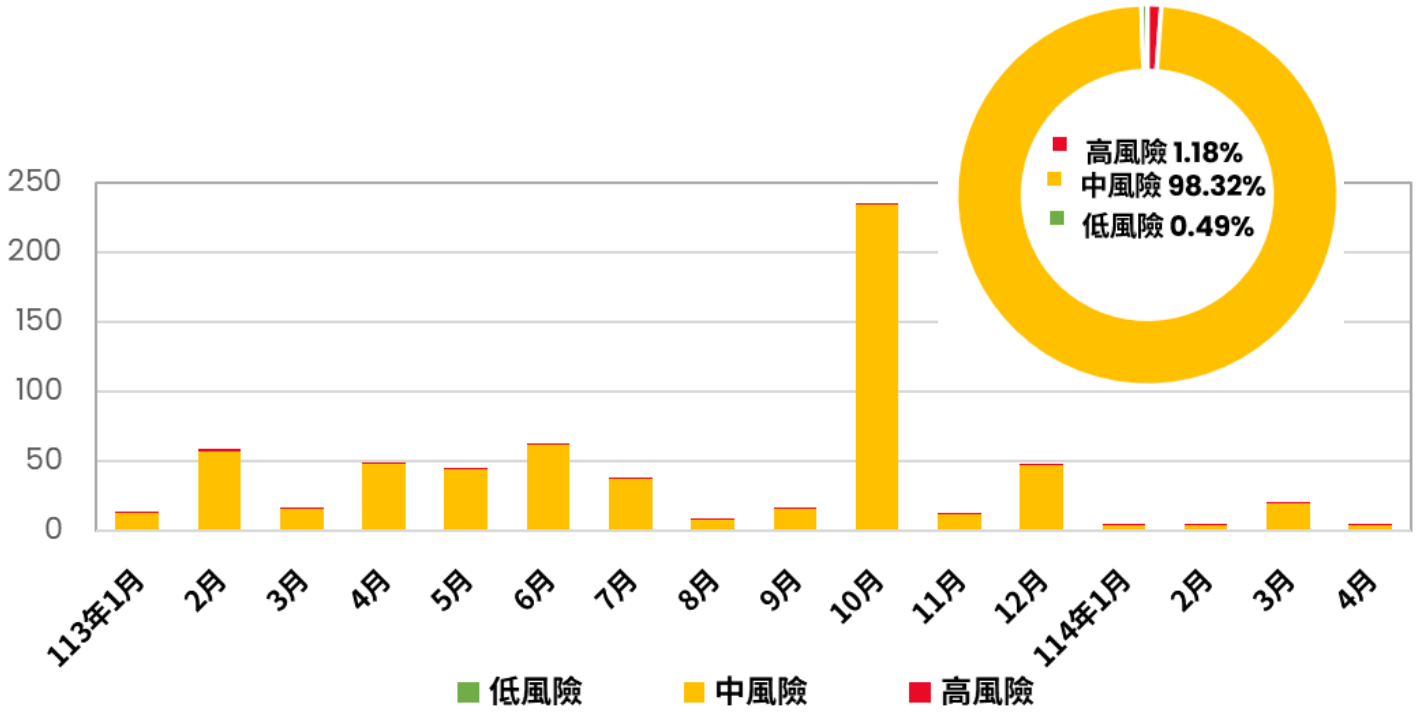
- 統計113年1月1日至114年4月30日政府機關攻擊分析發現並發布警訊通知之受駭情形，以感染殭屍網路佔30%為最多，勒索軟體偵測數量最少，推測勒索軟體攻擊者現行模式多以攻擊進入內網後散佈勒索軟體，取得利益最大化

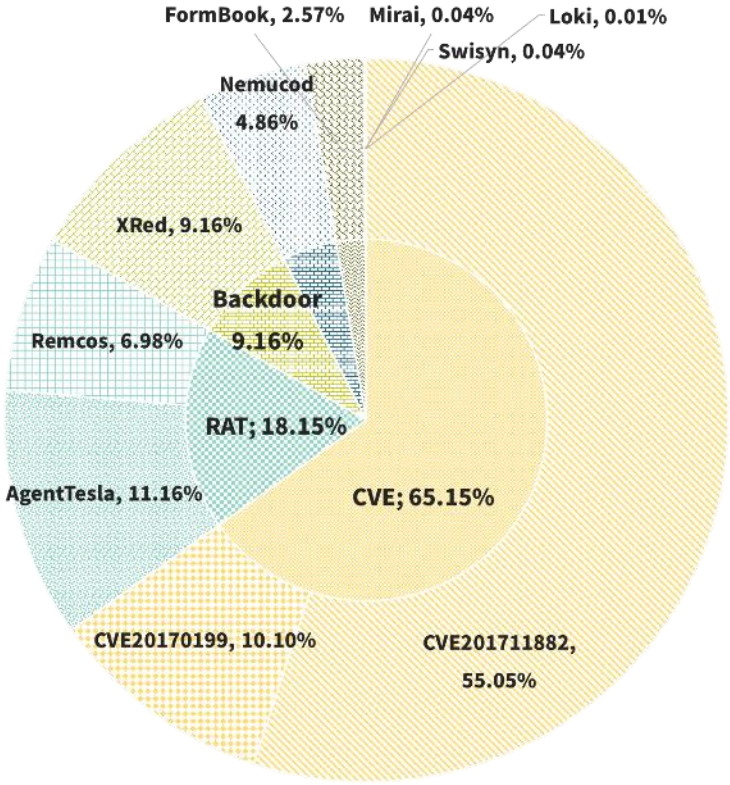


- 殭屍網路
  - 控制受駭設備成為殭屍節點，用以發動DDoS攻擊、散佈惡意程式、作為跳板橫向移動或進行進一步感染
- 後門/C2控制
  - 與遠端 C&C建立通道，供攻擊者遠端控制、植入其他工具或作為橫向跳板
- 惡意程式
  - 實施各類破壞或控制行為，如關閉防護、下載其他惡意模組、植入後門等
- 勒索軟體
  - 加密受駭者檔案、磁碟或系統設定後，要求支付贖金以換取解密金鑰
- 挖礦行為
  - 在背景悄悄執行加密貨幣挖礦，消耗受駭設備資源以獲取非法利益
- 資料竊取
  - 竊取瀏覽器憑證、帳號密碼、Cookies、系統金鑰、VPN 憑證等敏感資訊，並回傳至攻擊者C&C

惡意電子郵件分析(1/2)

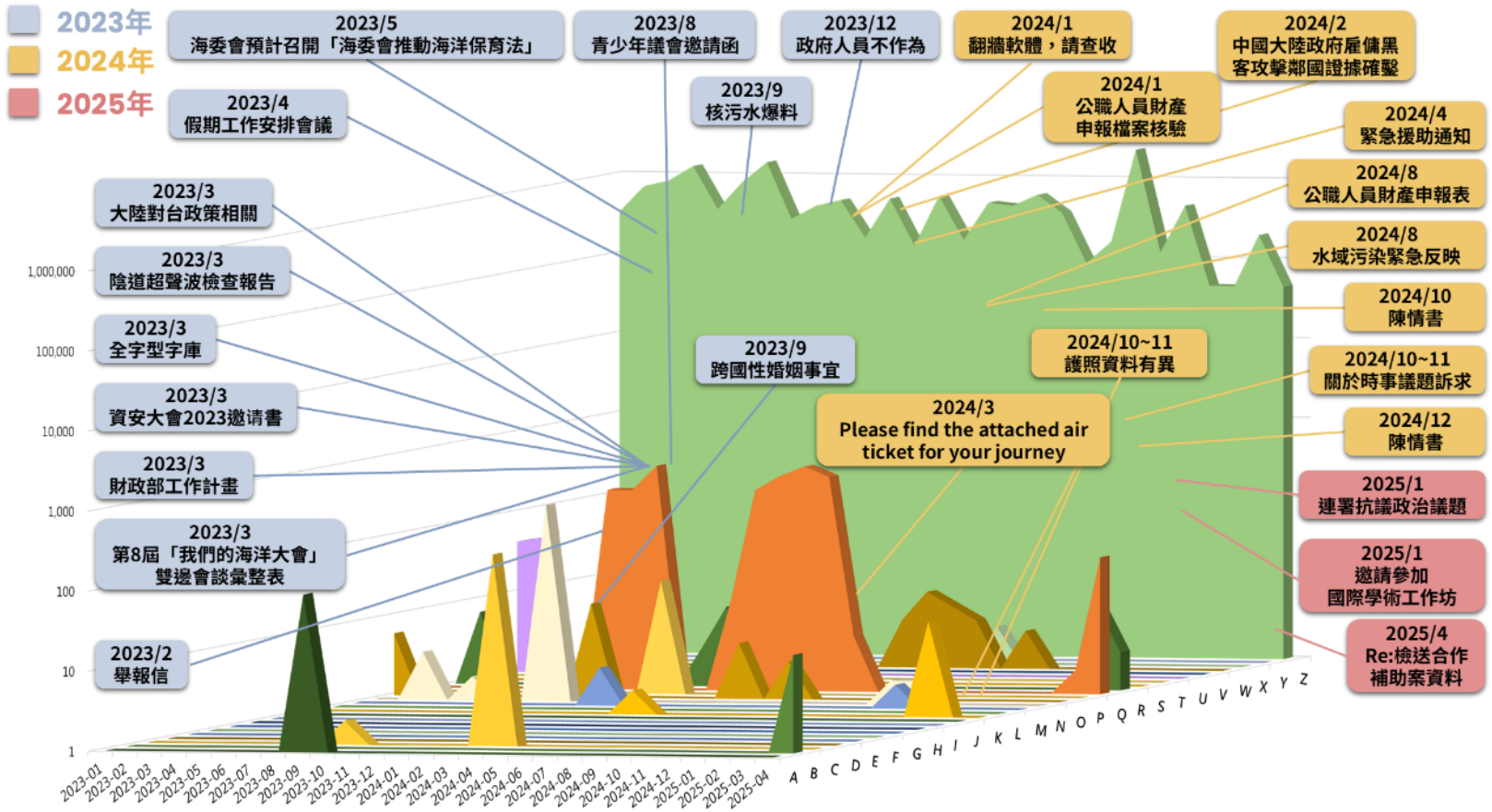
- 113年1月1日至114年4月30日偵測政府機關可疑惡意電子郵件，數量占總數的2.52%
- 含惡意附檔之郵件中，以散布CVE-2017-11882漏洞利用之惡意文件最多，其次則為遠端木馬AgentTesla與CVE-2017-0199漏洞





惡意電子郵件分析(2/2)

- 113年1月1日至114年4月30日政府領域APT郵件攻擊趨勢可歸納為11波攻擊行動，駭客利用公職人員財產申報、差旅訂票、檢舉爆料及補助案件合作等引誘性主旨，對政府機關人員發動攻擊

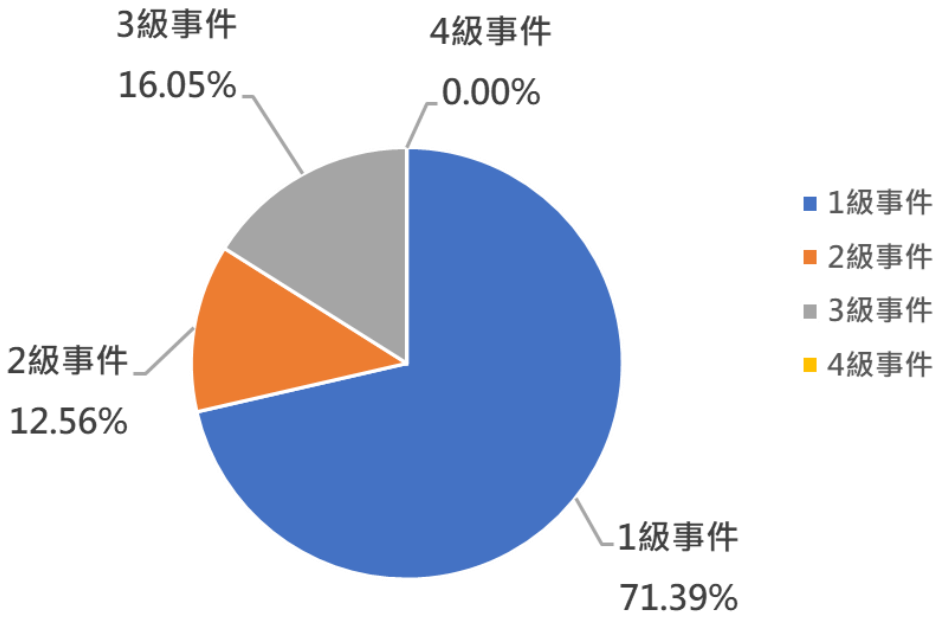


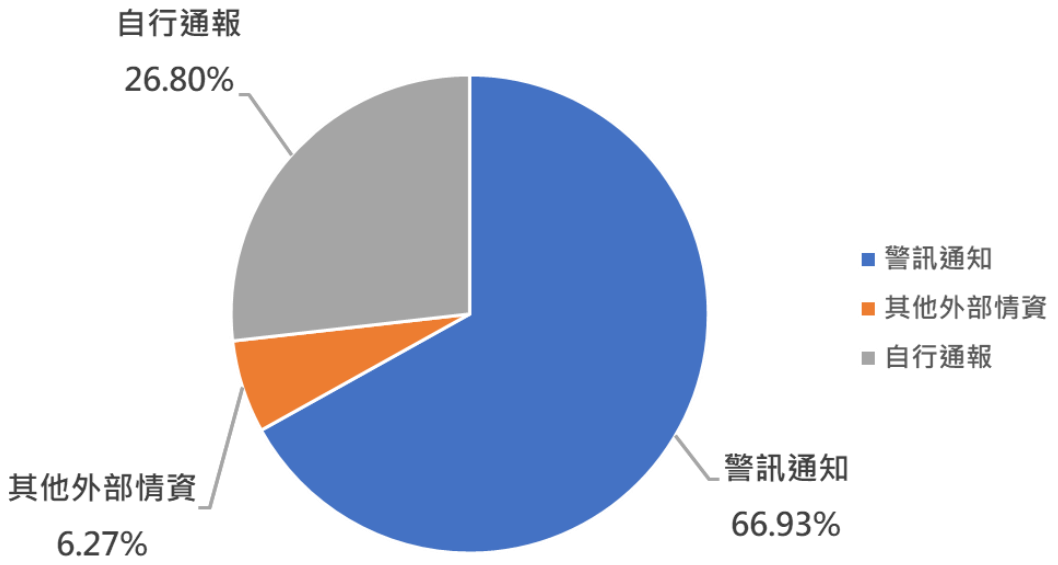
APT郵件攻擊手法

- 濫用合法郵件服務與使用者互動之多層式攻擊策略
- 以公職人員財產申報為由散布Star RAT遠端木馬程式
- 利用Office漏洞(CVE-2017-0199)搭配華航訂票相關主旨
- 利用MSC文件之新型態攻擊手法下載Cobalt Strike後門程式
- 透過RTLO手法搭配DLL Sideloading，並於郵件嵌入追蹤像素
- 利用內含惡意巨集之Word 文件，並搭配分段下載、動態解密等複合式技術

通報事件分析(1/2)

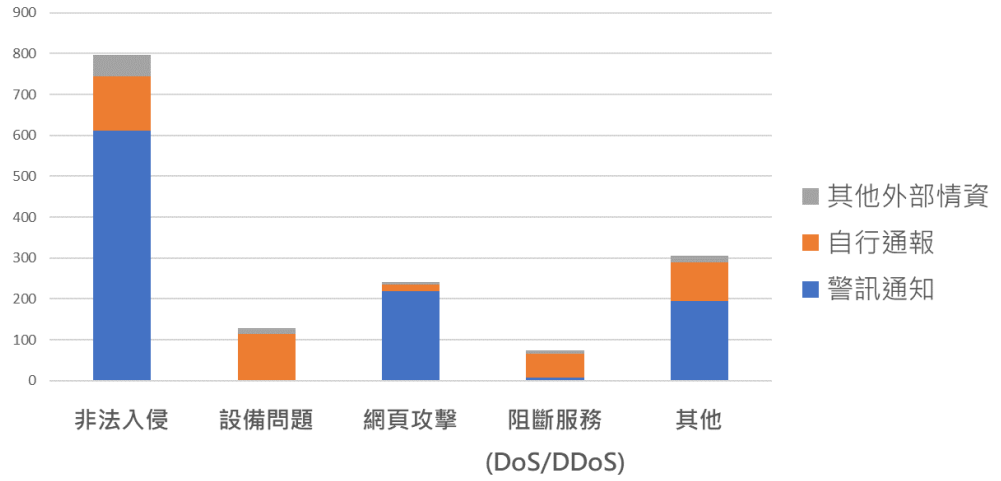
- 113年1月1日至114年4月30日接獲政府機關資安事件通報中，事件影響等級以 1級事件為主 占71.39%
- 66.93%為機關接獲資安院警訊通告後所進行之通報



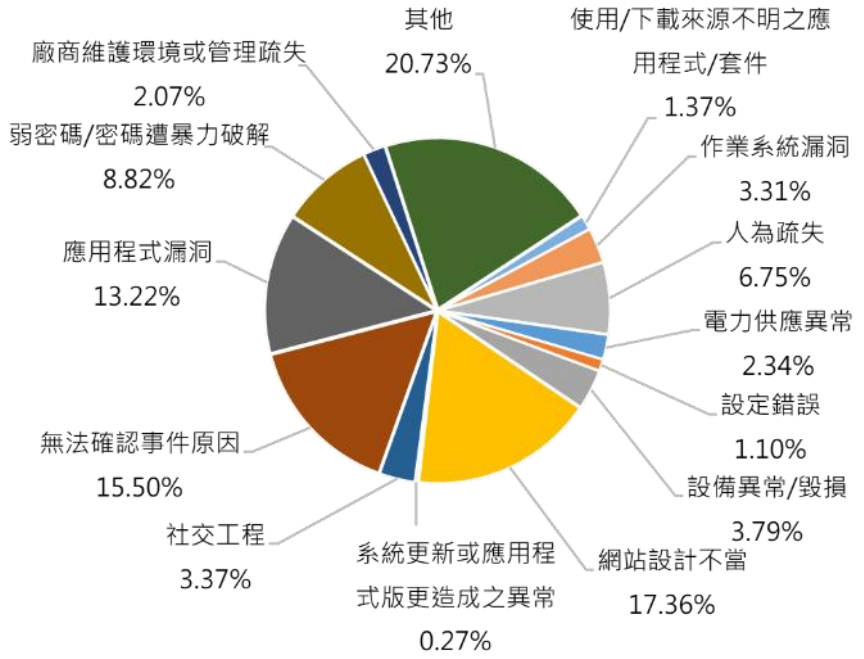


通報事件分析(2/2)

- 事件類型以 非法入侵 為大宗，其中又以 機關接獲資安院警訊通知 後進行通報為主



- 可識別之事件原因
  - 「網站設計不當」 17.36%
  - 「應用程式漏洞」 13.22%
  - 「弱密碼/密碼遭暴力破解」8.82%



國家資通安全研究院
National Institute of Cyber Security

政府資安事件案例分析

近期資安事件觀察

攻擊者註冊相似網域 散播冒牌通訊軟體，誘導使用者下載惡意程式

攻擊者 假借公務名義 進行社交工程攻擊，誘導至 外部網站/雲端平台下載惡意程式

權限與服務配置不當，過度暴露系統資源擴大攻擊面

設備風險管理不足，閒置設備與外來設備成為潛在入侵途徑

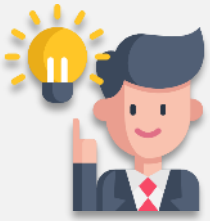
勒索軟體集團透過BYOVD攻擊手法，繞過防護機制

冒牌軟體安裝檔氾濫(1/2)

攻擊者註冊相似網域散播冒牌通訊軟體，誘導使用者下載惡意程式

案情提要

- 資安院偵測發現多個機關資訊設備疑似安裝冒牌軟體，產生Gh0st RAT惡意程式連線
- 調查發現同仁透過搜尋引擎查找Line安裝軟體，搜尋結果出現含有「line」字樣的.com網域之偽冒網站，致使用者誤認為官方下載頁面，安裝夾帶後門程式之Line安裝檔



防護建議

- 建立內部軟體下載與安裝相關規範，要求人員僅透過 官方網站 下載安裝程式
- 評估實施 應用程式白名單機制，禁止公務電腦安裝非授權軟體
- 公告與維護核可使用之公務使用軟體與載點，以制度化方式降低使用者操作風險

冒牌軟體安裝檔氾濫(2/2)

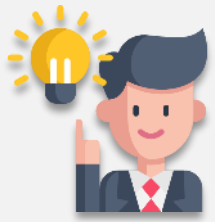
攻擊者註冊相似網域散播冒牌通訊軟體，誘導使用者下載惡意程式

社交工程攻擊手法多樣化(1/8)

瀏覽網站時不慎點擊下載並執行惡意程式

案情提要

- 某機關之電腦執行異常PowerShell指令，下載並執行惡意程式
- 調查發現該使用者瀏覽免費工具網站，配合網站引導進行「我不是機器人驗證」，誘導使用者 手動操作執行PowerShell指令，導致使用者下載並執行竊資程式



防護建議

- 建議機關啟用PowerShell日誌記錄功能，並結合EDR與 SIEM即時監控異常活動，以即時偵測並攔截可疑行為
- 加強社交工程攻擊手法之宣導訓練，提升使用者對誘導輸入 系統指令之警覺性

按下按鈕後，該網站會將惡意指令碼放入剪貼簿

社交工程攻擊手法多樣化(2/8)

以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式

案情提要

案例1

- 資安院發現駭客寄送以「稅務調查」為由之社交工程電子郵件給政府機關人員
- 部分政府機關人員接獲信件後，信以為真，打開信件附件後，連至 附件中提供之外部下載連結下載檔案，導致電腦受駭

社交工程攻擊手法多樣化(3/8)

以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式

案例1

中華民國 財政部 Ministry of Finance, R.O.C.

【114】財政部

114年稅務稽查抽查結果公示

根據《中華民國政府資訊公開條例》、《國稅局關於印發<推進稅務稽查隨機抽查實施方案>的通知》（【114】年財政部）的要求，現將隨機抽查結果公示如下：

隨機抽查方式

市稅務稽查雙隨機工作平台內重點稽查對象名錄庫、異常稽查對象名錄相關企業

隨機抽查方式定向或不定向抽查的方式，透過稅務稽查雙隨工作平台抽取。其他

事項

對抽取的稽查對象 113 年至 114年的稅務義務履行及其他稅法遵從情況進行檢查，如發現重大稅務違法行為線索，可向前追溯或向後延伸，請及時通知財務稅務負責人

配合稅務局檢查稅務專員完成相關抽查工作。 （註：用電腦版開啟）

國稅局 114年度稅務稽查隨機抽查企業名單公佈：

各企業單位請下載自我查詢

點選下載查詢

https://rgghrt1140120-1336065333.cos.ap-guangzhou.myqcloud.com/查閱1140120.zip

超連結指向託管惡意檔之雲端硬碟網址

社交工程攻擊手法多樣化(4/8)

以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式

案情提要

案例2

- 攻擊者利用 官網民意信箱/陳情管道，要求業務承辦人自 Google 雲端硬碟連結下載壓縮檔案，且提供檔案密碼
- 當承辦人依要求下載並解壓縮檔案，再點擊偽 裝成 PDF 文件之捷徑檔(LNK)後，惡意程式即遭載入並執行

郵件主旨：【與申訴/陳情相關】

寄信信箱：【盜用之公務信箱/免費信箱】

信件內容：

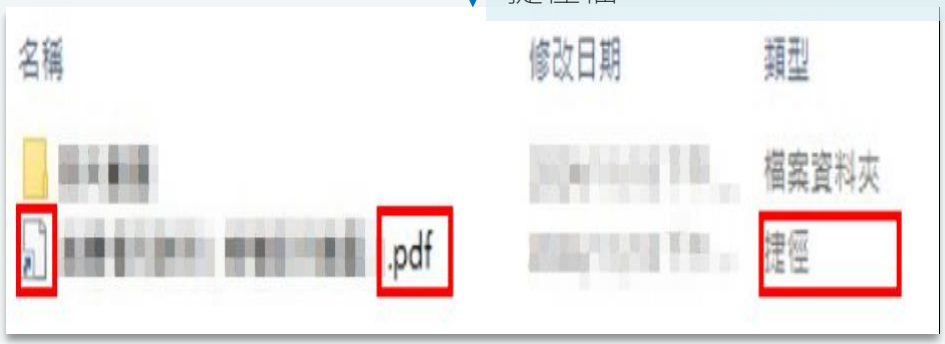
【提供雲端空間下載連結】

https: //drive.google.com/…=drive_link

壓縮檔密碼 OOOOOO

檔案解壓縮後，誘導使用者點擊偽裝成PDF文件之捷徑檔

常見格式



社交工程攻擊手法多樣化(5/8)

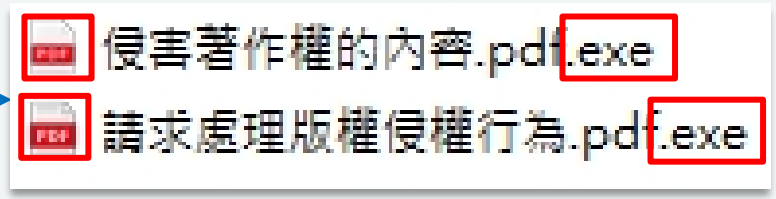
以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式

案情提要

案例3

- 攻擊者以版權侵權為由，假冒企業的法律部門，寄送帶有偽裝成PDF檔案附件的釣魚信，引誘使用者下載並執行惡意程式
- 機關同仁接獲主旨為「版權侵權通知」的信件，下載並執行檔案後，電腦遭植入竊資軟體

看似pdf檔，實際上是文字超連結，連結以下載壓縮檔



檔案解壓縮後，誘導使用者點擊偽裝成PDF文件之執行檔

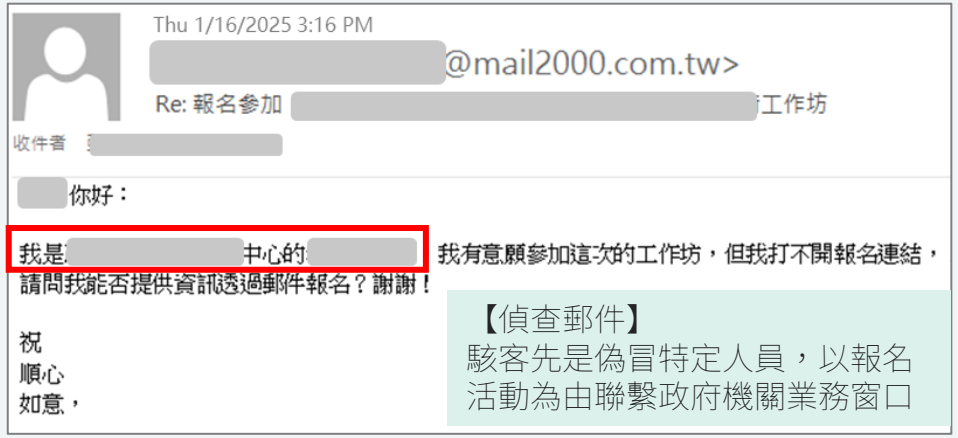
社交工程攻擊手法多樣化 (6/8)

以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式

案例4

案情提要

- 攻擊者利用遭駭之Mail2000個人信箱與公司信箱，寄送與會議邀請或公務合作相關之正常無害電子郵件，待受駭者回覆郵件後，再寄送惡意檔案或設定雲端惡意檔案存取權限給受駭者
- 透過多層次社交工程電郵攻擊手法，取得受駭者信任，提高攻擊成功率，以達到成功竊取受駭者電腦資訊之目的



【偵查郵件】
駭客先是偽冒特定人員，以報名活動為由聯繫政府機關業務窗口

【魚叉式攻擊】
待業務窗口回覆郵件，駭客確認其為有效收件人，以無法填寫表單為由，附上惡意檔案發動攻擊

社交工程攻擊手法多樣化(7/8)

以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式

案情提要

案例5

- 某機關發現電腦執行不明程式，並對外產生異常連線
- 調查發現攻擊者透過 求職網傳送之履歷 夾帶惡意附件
- 同仁因業務需求下載附件，發現疑似Excel試算表之檔案，惟該檔案實際上係 Excel外掛元件(XLL)可執行檔，同仁執行檔案後，即觸發惡意程式執行，致電腦遭入侵並對外異常連線

履歷

姓名：王O明

手機：09XX-XXX-XXX

Email：OOO@gmail.com

工作經歷：

2022/05 – 至今 資訊助理工程師

2020/03 – 2022/05 研究助理

…

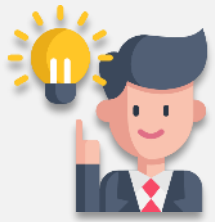
附件

下載檔案　檔案夾帶惡意XLL檔

求職網

社交工程攻擊手法多樣化(8/8)

以公務名義發動社交工程攻擊，誘導使用者至外部網站/雲端平台下載惡意程式



防護建議

- 強化內部人員資安教育訓練，提升對新興攻擊手法之辨識與應對能力
- 針對信件中附有加密壓縮檔或外部雲端下載連結提高警覺，避免輕信點擊
- 檢視外部檔案前應先以防毒軟體掃描，並於沙箱或隔離環境中處理高風險檔案
- 開啟檔案前應確認其 實際檔案類型，特別留意捷徑(.lnk)或應用程式(.exe)等可執行檔，避免因檔名或圖示誤導而執行惡意程式
- 建議啟用「顯示副檔名」功能，以清楚辨識檔案實際類型，避免因檔名或圖示誤判

網通設備弱點暴露(1/3)

SonicWall網通設備漏洞暴露

案情提要

案例1

- SonicWall旗下網通設備作業系統SonicOS於114年1月遭揭露存在高危風險漏洞，可使駭客遠端繞過身分驗證，劫持使用中SSL VPN session 存取單位私有網路
- 政府領域共64個機關(67個IP)使用之SonicWall網通設備存在此漏洞風險，多數為D級綜合行政類機關。資安院已針對相關高風險之機關發布警訊，並提供相關防護建議進行風險緩解

漏洞編號	CVE-2024-53704
漏洞分數 (CVSS 3.1)	9.8(CRITICAL)
漏洞類別	不當身分驗證 (Improper Authentication)
受影響版本	• Gen7 Firewalls系列產品型號：TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 (7.1.1-7058(含)以前版本與7.1.2-7019版本) • Gen7 NSv系列產品型號：NSv 270, NSv 470, NSv 870 (7.1.1-7058(含)以前版本與7.1.2-7019版本) • TZ80(8.0.0-8035版本)

資料來源：資安院整理

UPDATE: Proof-of-Concepts (PoCs) for the SonicOS SSLVPN Authentication Bypass Vulnerability (CVE-2024-53704) are now publicly available. This significantly increases the risk of exploitation. Customers must immediately update all unpatched firewalls (7.1.x & 8.0.0). If applying the firmware update is not possible, disable SSLVPN. For further assistance, please contact SonicWall support.

資料來源：SonicWall Security Advisory (SNWLID-2025-0003)

網通設備弱點暴露(2/3)

Fortinet網通設備漏洞暴露

案情提要

案例2

- Fortinet官方分別於114年1月與2月揭露旗下網通設備作業系統FortiOS與安全網頁閘道器FortiProxy之網頁管理介面存在高危風險漏洞，可使駭客遠端繞過身分驗證，獲得超級管理者權限
- 經研析發現，政府領域共22個機關(25個IP)使用之Fortinet網通設備存在此漏洞風險，多數為C級綜合行政類機關。資安院已針對相關高風險之機關發布警訊，並提供相關防護建議進行風險緩解

漏洞編號	CVE-2025-22457
漏洞分數(CVSS 3.1)	9.8(CRITICAL)
漏洞類別	越界寫入(Out-of-bounds Write)
受影響版本	• Ivanti Connect Secure 22.7R2.5(含)以下版本 • Pulse Connect Secure (已不支援) 9.1R18.9(含)以下版本 • Ivanti Policy Secure 22.7R1.3(含)以下版本 • Ivanti Neurons for ZTA gateways 22.8R2(含)以下版本

資料來源：資安院整理

An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS and FortiProxy may allow a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module or via crafted CSF proxy requests.

Please note that reports show this is being exploited in the wild.

資料來源：FortiGaurd Labs PSIRT Advisory (FG-IR-24-535)

網通設備弱點暴露(3/3)

Ivanti網通設備漏洞暴露

案情提要

案例3

- Ivanti於114年2月揭露旗下相關網通設備存在高危風險漏洞，駭客可惡意利用漏洞觸發越界寫入，並導致遠端程式碼執行
- 政府領域共12個機關使用之Ivanti網通設備存在此漏洞風險，多數為B級機關。資安院已針對相關高風險之機關發布警訊，並提供相關防護建議進行風險緩解

漏洞編號	CVE-2025-22457
漏洞分數(CVSS 3.1)	9.8(CRITICAL)
漏洞類別	越界寫入(Out-of-bounds Write)
受影響版本	• Ivanti Connect Secure 22.7R2.5(含)以下版本 • Pulse Connect Secure (已不支援) 9.1R18.9(含)以下版本 • Ivanti Policy Secure 22.7R1.3(含)以下版本 • Ivanti Neurons for ZTA gateways 22.8R2(含)以下版本

資料來源：資安院整理

防護建議

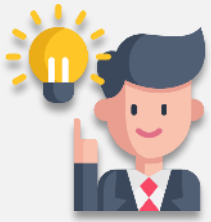
- 針對所有使用產品之設備，應盤點版本狀態並依照官方公告盡速更新至最新版本
- 若無法立即更新，建議採取臨時緩解措施（如封鎖特定連接埠、禁用可疑模組等），以降低漏洞可利用風險

權限與服務配置不當(1/2)

未妥善管理雲端平台檔案存取權限，導致敏感資料存在外洩風險

案情提要

- 機關於辦理活動期間，將活動簡章存放於Google 雲端空間供民眾下載，惟承攬廠商亦將 包含個人資料之報名者資訊 上傳至該雲端空間，且 存取權限設定未臻完善 ，致未授權之使用者得以存取相關資料，導致民眾個人資料外洩事件



防護建議

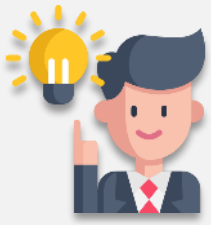
- 使用雲端空間儲存資料時，應確保公開文件與涉及個人資料之檔案 存放於不同雲端目錄或獨立儲存空間，同時 設定適當存取權限，以防範未經授權之第三方存取或下載
- 委託廠商辦理活動時，應於合約中 明訂個人資料保護責任，包含資料存放方式、存取限制、保存期限及刪除機制等，並於活動結束後即辦理個人資料移除或歸檔作業，不得將個資存放於雲端儲存空間，以降低個人資料外洩風險

權限與服務配置不當(2/2)

遠端存取缺乏控管，導致多台系統遭入侵

案情提要

- 某機關系統維護廠商為方便維護管理作業，於網站主機上 安裝遠端桌面軟體(AnyDesk)，惟 未搭配防火牆白名單、存取限制等控管機制
- 攻擊者透過AnyDesk遠端連線主機，暴力破解密碼登入後，透過遠端桌面通訊協定(RDP)橫向滲透至 Active Directory(AD)主機，進一步利用AD對內部電腦部署並執行惡意程式，導致多台設備受駭

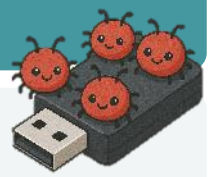


防護建議

- 依資通安全管理法施行細則第4條落實委外監督管理之責，確保資安防護措施之有效性
- 委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理
- 存取控制採 最小權限原則，僅依機關業務需求，開放指派任務所需之授權存取

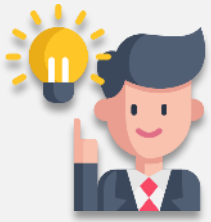
閒置與外來設備成為潛在資安風險(1/2)

外接裝置成入侵媒介



案情提要

- 資安院偵測發現某機關資訊設備產生蠕蟲程式特徵之異常連線
- 經機關調查，研判感染源為 外部廠商使用之USB裝置；廠商透過該USB 裝置協助機關同仁安裝印表機驅動程式，進而導致感染



防護建議

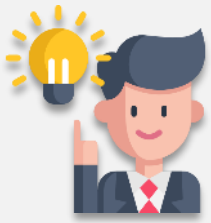
- 外部廠商應遵守單位作業管理流程，落實資訊設備各項檢查作業
- 應建立單位可攜式媒體安全使用守則，降低使用外部設備之風險，如：使用外部設備前，應先執行病毒掃描與檢測

閒置與外來設備成為潛在資安風險(2/2)

歷史系統未妥善下架與管理，致敏感資料外洩

案情提要

- 某機關網站已於十多年前關閉前台服務，惟其連接的資料庫未同步下架或移除，且持續可由外部網路連線存取
- 近期，該機關接獲外部情資指出該網站資料疑似外洩。調查研判攻擊者發現並連線進入該遺留資料庫後，竊取存放之個人資料



防護建議

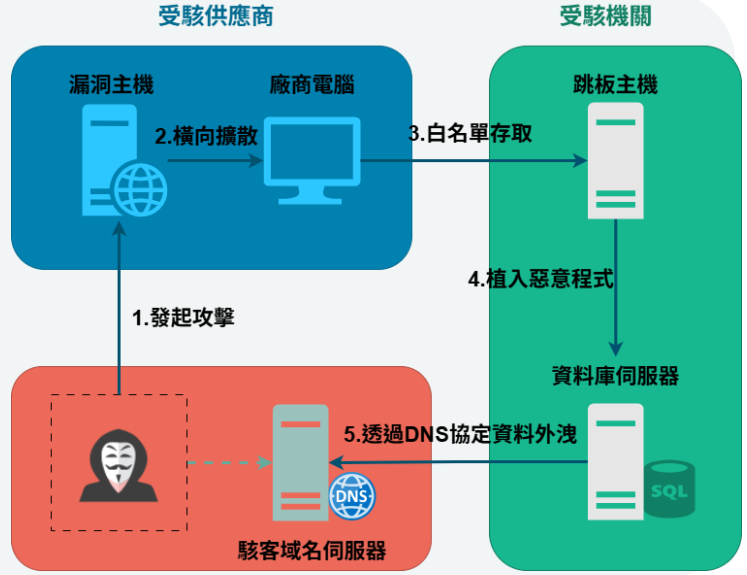
- 建立並落實網站上/下線相關作業程序，確保關閉系統後相關資源亦同步移除
- 定期執行 資產盤點與弱點掃描，以發現未管理之遺留系統與服務
- 政府機關應遵循「個人資料保護法」相關規定，對於敏感個資採取嚴謹資料管控措施，確保蒐集之個人資料不會外洩、竄改或不當使用

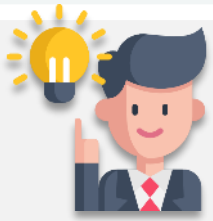
廠商供應鏈橫向移動

機關供應鏈廠商遭駭，橫向移動機關內部，DNS Tunnel報到

案情提要

- 駭客利用供應商端主機漏洞作為入侵起點，避開直接攻擊受駭機關的防線
- 供應商內部進行橫向移動，逐步掌握更多資源並尋找對外可用跳板，藉由跳板機對機關進行白名單連線，躲避監控與偵測
- 成功滲透至內部網路後入侵資料庫伺服器，部署惡意程式建立持續控制
- 駭客使用偽冒chatgpt網域透過DNS Tunnel進行資料外洩





防護建議

- 強化第三方存取管控與跳板機連線驗證機制，僅提供廠商必要性權限帳號存取
- 部署相關防護偵測機制，監控和限制橫向移動工具的使用，部署端點與內網攻擊偵測機制，針對應盡速處理告警，減輕受駭程度

勒索軟體繞過EDR防護(1/2)

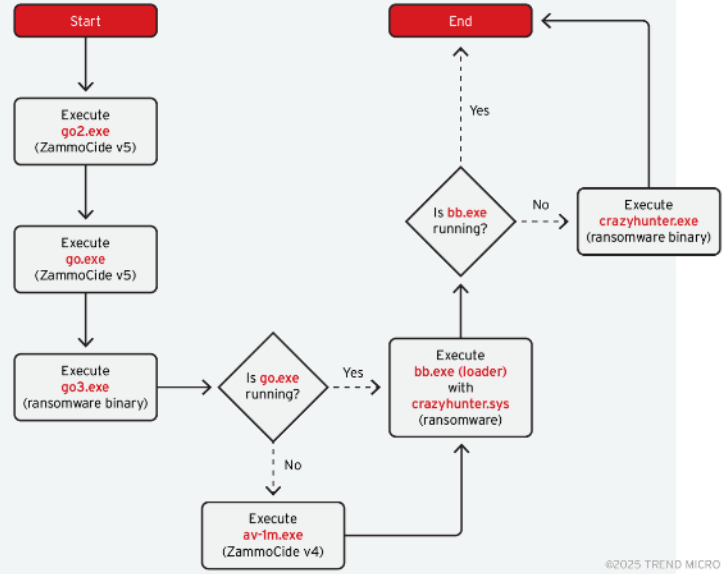
CrazyHunter攻擊臺灣醫院，自帶驅動程式(BYOVD)手法迴避偵測

案例1

案情提要

- CrazyHunter，被揭露組織約有8成的作案工具透過GitHub平臺取得，並透過自帶漏洞驅動程式(BYOVD)手法迴避偵測
- 攻擊公眾面向服務，取得權限後向後探測AD取得管理者權限，透過開源工具執行攻擊活動
- 自帶漏洞驅動程式BYOVD規避偵測，並關閉端點防護
- 透過受信任域名之基礎設施執行C&C資料洩漏活動，難以偵測

```
eventSubId: 402 AND objectRegistryKeyHandle: ZammOcide AND
objectRegistryData: zam64.sys
```



資料來源：CrazyHunter Campaign Targets Taiwanese Critical Sectors | Trend Micro (US)

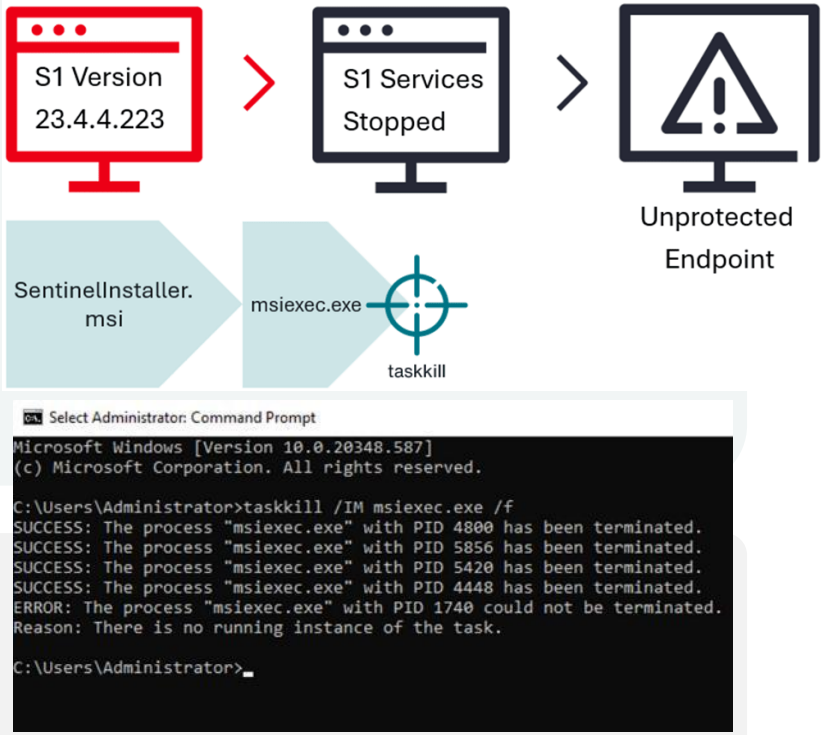
勒索軟體繞過EDR防護(2/2)

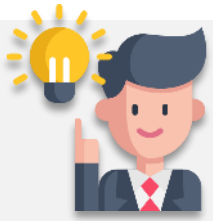
Babuk運用EDR合法安裝，自帶驅動程式(BYOVD)手法迴避偵測

案例2

案情提要

- 勒索軟體Babuk攻擊的資安事故裡，發現駭客濫用EDR合法安裝程式的新型態手法，藉由本機升級或降級Agent，而能終止現有Agent的運作
- 駭客使用自帶漏洞驅動程式（Bring Your Own Vulnerable Driver，BYOVD)攻擊手法繞過防護
- 端點防護能提升資安防護，但仍有被繞過的可能性，其他資安防護仍然重要





防護建議

- 建立驅動程式白名單等驅動安裝監控機制，防止駭客透過合法簽章漏洞驅動程式滲透系統核心
- 落實權限控管，降低惡意驅動安裝風險

資料來源：Bring Your Own Installer: Bypassing EDR Through Agent Version Change Interruption

國家資通安全研究院
National Institute of Cyber Security

政府機關資安防護強化重點

謹慎對待社交工程攻擊

不隨意點擊可疑連結、登入偽造網站

- 如需登入系統操作（Webmail、內部系統等）請主動前往系統確認
- 勿點擊信件、社群平台、簡訊中的縮網址或不明連結，甚至輸入帳號密碼等資訊

仔細辨識來路不明的信件與附件

- 確認信件寄信內容是否合理，若有附件或超連結，應更謹慎確認，再決定是否開啟
- 檢視外部檔案前應先以防毒軟體掃描，並於沙箱或隔離環境中處理高風險檔案

養成求證與通報的習慣

- 遇公務信件存可疑內容應向寄件人求證內容，特別是有附件或超連結之信件
- 若遇社交工程信件，應可向資安專責人員通報，預防更多受駭情形

落實資產設備管理防護

落實資產管理與弱點修補

- 定期盤點機關資訊設備，及時進行漏洞修補與安全性更新
- 無更新支援之設備應強化資安控制措施，並盡速規劃汰換

妥善管理設備存取系統控制

- 定期檢視系統設備之帳號，存取權限，定期更換密碼，符合密碼複雜性原則
- 定期檢視網路架構與設備設定，確保內部系統與服務不曝露於網際網路中

留意多方來源弱點威脅情資

- 追蹤資安新聞與漏洞通報資訊，CISA、NVD 及主要資安媒體快訊，以利確認使用設備、作業系統或應用服務是否有弱點漏洞，並及時修補

預防供應鏈受駭與橫向移動

強化第三方廠商存取權限與行為審核

- 僅提供廠商必要性最小權限且具合理時效性的帳號存取，並可採用多因子驗證
- 對廠商維運通道建立「存取審核機制與記錄留存」，定期進行帳號清查與異常行為檢測

部署防禦橫向移動之相關偵測機制

- 監控和限制橫向移動工具的使用，部署端點與內網攻擊偵測機制，提高偵測異常行為及早防禦攻擊
- 針對SOC監控團隊提出之內網橫向移動告警，應盡速處理，減輕受駭程度

針對軟體與驅動程式建立控制機制

- 建立白名單策略，僅允許經過審核之軟體驅動程式安裝與執行，
  阻擋任何未授權名單內的第三方軟體與驅動程式

結論與建議

結論與建議

- 當前資安威脅環境日趨嚴峻，不論是個人資料或機關憑證，一旦外洩將直接破壞既有防護機制；大量應用轉向雲端卻未妥善配置，更衍生多重風險。設備與軟體弱點揭露頻率升高，社交工程與勒索軟體攻擊橫行，供應鏈攻擊事件更撼動邊界信任，駭客甚至結合 AI 技術加速滲透與詐騙手法演進
- 本院透過蜜罐技術觀測全球攻擊行為發現，網頁應用服務仍為駭客掃描重點，其中尤以殭屍網路活動最為活躍。政府聯防監控亦觀察到，駭客逐漸結合防毒禁用、程式混淆等手法，規避既有防護以提高入侵成功率
- 政府機關攻擊分析顯示，遭駭裝置仍以伺服器與個人電腦為主，亦包含 NAS、無線 AP、網路分享器等邊緣設備。社交工程信件雖仍利用舊漏洞，但多以引誘點擊之議題為誘因。通報事件中，非法入侵類型比例最高，且多數與網站設計不當有關
- 近期多起勒索軟體攻擊事件接連發生，無論是針對公部門或私人企業，駭客入侵手法皆趨向多樣化，可能來自公眾服務、設備弱點，甚至供應鏈滲透。不僅挑戰資安架構的完備程度，更凸顯出資安人員在入侵後告警階段的處置效率關鍵。唯有擺脫對單一防護機制的過度依賴，持續檢視潛在弱點漏洞與加速應變，才能在攻擊來臨時守住防線，降低衝擊

國家資通安全研究院
National Institute of Cyber Security

Thank you for your time.

報告完畢
敬請指教

簡報人員- 姓名 職稱