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

政府機關資安威脅與防護重點

國家資通安全研究院
通報應變中心

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

全球資通安全威脅趨勢

全球資通安全威脅趨勢

- 綜整113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

個人資料與憑證外洩致防護機制失效

雲端應用服務衍生多元威脅

社交工程泛濫致APT鎖定與勒索軟體風險增加

資通系統弱點頻遭揭露利用

資安(訊)供應鏈駭破壞邊界防護

關鍵資訊基礎設施與OT攻擊面向增加

發令與控制

採取行動

個人資料與憑證外洩致防護機制失效

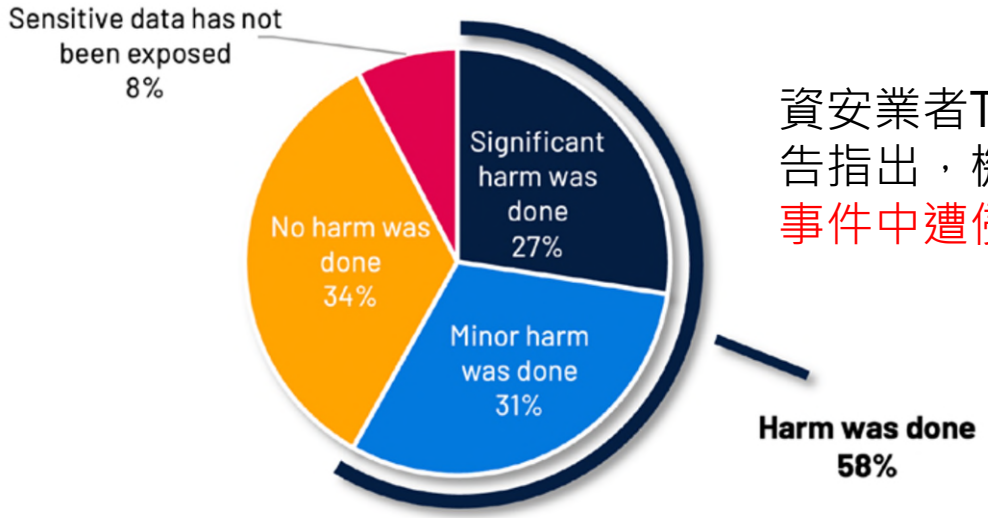
- IBM X-Force Threat Intelligence Index 2024 使用有效憑證之攻擊量逐年增加，濫用有效帳戶入侵已成為網路犯罪者最常見之切入點，占 X-Force 所有事件的 30%
- IBM 113年資料外洩成本報告 (Cost of a Data Breach Report 2024)調查顯示，資料外洩於112年平均成本高達488萬美元，相較112年增加10%，資料外洩平均成本呈現年年增長趨勢，成本大幅飆升的原因為業務中斷損失與事件發生後的客戶支援與補救措施
- 資料外洩3個根因
  - 惡意攻擊，由外部攻擊者或內部犯罪者實施之攻擊占所有違規行為55%
  - 23% 是 IT 故障
  - 22% 是由於人為錯誤造成

70% 組織遭遇外洩事件時，自認對業務造成重大或非常重大的侵擾。只有 1% 的人表示破壞程度較低

圖片來源: https://www.ibm.com/downloads/cas/1KZ3XE9D

雲端應用服務衍生多元威脅

- 資安廠商Thales 113年Global Threat Report報告指出，從 111 年到 112 年，雲端環境入侵增加 75%，其中攻擊者鎖定雲環境而入侵者案例增加 110%，未意識到是針對雲入侵，但連帶侵害到雲環境之案例增加 60%
- Cloud Security Alliance (CSA)雲端安全聯盟提出113年前5大雲端環境威脅
  - 組態錯誤與不適切之變更控制
  - 身分存取管理失當
  - 不安全的介面與APIs
  - 雲端安全策略選擇或實施不充分
  - 不安全的第三方資源



資安業者Tenable雲端安全報告指出，機敏資料幾近6成於事件中遭侵害

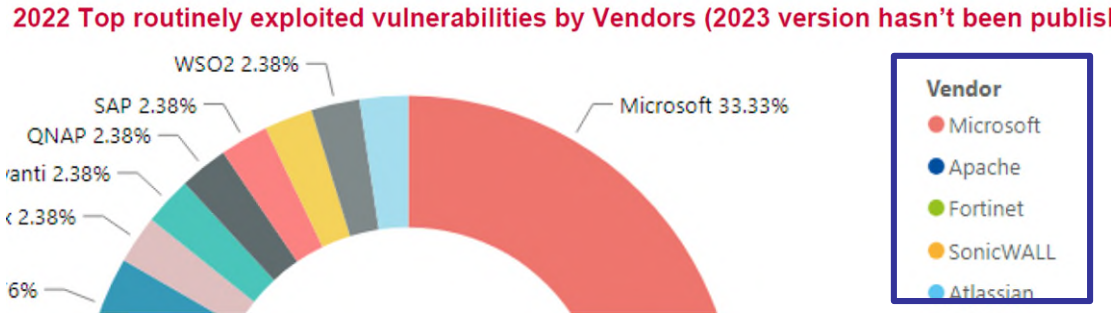
圖片來源: https://static.tenable.com/marketing/research-reports/ResearchReport-2024_Cloud_Security_Outlook.pdf

社交工程泛濫致APT鎖定與勒索軟體風險增加

- ENISA113年威脅全景報告(統計期間112年7月至113年6月)指出，阻斷式服務(DDoS)與勒索軟體攻擊位居榜首，商業電子郵件侵害 (BEC) 事件急劇增加
- 微軟威脅情資團隊揭露，駭客組織Black Basta 集團使用Microsoft Quick Assist 透過網路釣魚語音電話 (Vishing) 發動社交工程攻擊、部署遠端監控與管理 (RMM) 工具及植入惡意程式，並散播勒索病毒
- 資安廠商Verizon113年資料外洩調查指出，透過電子郵件進行網路釣魚與偽冒電話或簡訊仍是發生網路安全事件之主要原因，約占社交工程事件之73%；數據亦顯示遭受社交工程電子郵件釣魚者，落入陷阱時間平均少於1分鐘
- ENISA提醒由於生成式人工智慧之使用已經標準化，生成式文字、圖像、音訊及視訊仿真度大幅提高。生成式AI支援客製化之網路釣魚活動，將提供更令人信服之誘餌

資通系統弱點頻遭揭露利用

- ENISA113年威脅全景報告(統計期間112年7月至113年6月)共發現19,754 個漏洞，其中9.3% 屬於「嚴重」類別，21.8% 屬於「高」
- 資安廠商Action1公布113年軟體漏洞評估報告，揭露以下趨勢
  - 負載平衡器正成為一個有吸引力的目標，其遭利用率創歷史新高，值得注意的數據為NGINX (100%) 與 Citrix (57%) 之利用率
  - 蘋果作業系統越來越受到攻擊者的關注，112年蘋果作業系統 MacOS 與 iOS 的利用率分別增加 7%與 8%
  - MSSQL遠端程式碼執行(RCE) 漏洞激增 1600%，突顯新漏洞利用風險激增，112年嚴重漏洞(Critical Vulnerabilities)高達17個
  - MS Office 使用者增加，突顯攻擊者利用人為錯誤之弱點。辦公室應用程式中，Microsoft Office 漏洞總數預計最高，其中 40%~50% 是RCE，利用率為7%，高於111年2%



供應商弱點排名

圖片來源 :https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

資安(訊)供應鏈遭駭破壞邊界防護

- 113年供應鏈重大資安事件：113年7月時CrowdStrike Falcon EDR更新錯誤造成微軟當機事件，數以百萬計資通系統遭受影響，且使相關業務服務因此停頓，CrowdStrike亦面臨客戶跟投資者之賠償請求；微軟於10/22發出警告，7月導致全球藍色螢幕當機(BSOD)之 CrowdStrike，其Falcon EDR軟體會導致某些程式在 Windows 11 24H2 中出現停止運作，其中包括常用的 Microsoft Excel 與 Word
- 資安廠商ReversingLabs偵測到透過開源套件傳播威脅增加 1,300% 以上，2020 年至 2023 年間，PyPI 平台上發現的威脅數量僅在 2023 年就增加400%

新的 Python 漏洞可規避傳統應用程式安全工具的偵測

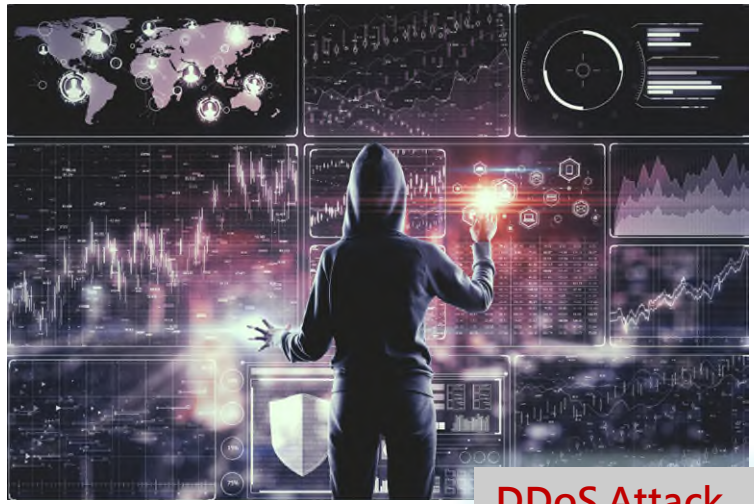
圖片來源:
file:///D:/2024%20Project/%E5%B9%B4%E5%A0%B1/ref/The-State-of-Software-Supply-Chain-Security-2024.pdf

關鍵資訊基礎設施與OT攻擊面向增加

- 資安廠商Sophos 在2024 年關鍵基礎設施勒索軟體現況指出，能源、石油/天然氣及公用事業(62%)是遭受攻擊影響之設備比例最高產業；其次是醫療保健產業 (58%)，入侵手法首位是利用系統漏洞，占49%；其次是洩漏的憑證，有超過四分之一 (27%)攻擊中使用
- 113年10月，美國水務公司 (American Water)遭遇網路攻擊，攻擊涉及未經授權存取美國水務公司之電腦網路與系統，其可能影響範圍超過 1400 萬人遍及 14 個州與 18 個軍事設施
- 113年8月，俄飛彈與無人機夜襲烏克蘭攻擊能源基礎設施，引發大火，導致空氣中氯含量上升，造成72個城鎮等定居點與1萬8,500多名居民停電

暗潮洶湧：DDoS來襲

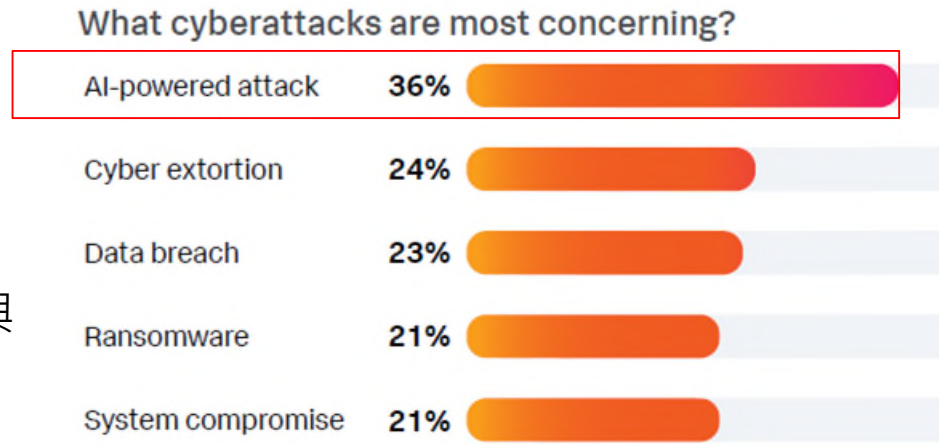
- 自新冠疫情開始、直至俄烏戰爭到最近以哈、伊朗及台灣、中國等衝突或緊張局勢，觀測從111年基於政治動機所展開之DDoS攻擊開始捲土重來，主要目的為藉由耗盡系統、服務及其相關資源或使網路基礎設施超載，以阻斷可用性
- 根據 Microsoft 報告顯示，其全球DDoS減緩團隊平均每天對抗 1,700 次攻擊，另一家資安廠商NETSCOUT則統計，112年全球有超過 1,300 萬次DDoS攻擊
- Cloudflare於112年第 4 季觀測，由於台灣大選接近及與中國之緊張情勢，針對台灣的 DDoS 攻擊流量較去年同期相比增加 3,370%。113年第 1 季偵測 450 萬次DDoS 攻擊，比去年成長50%
- DDoS出租平台助長攻擊增加，據Microsoft統計，觀測單單111年即成長20%
- StormWall 統計112年前 3 名DDoS 攻擊影響最嚴重的領域，分別為金融、政府服務及零售業者 ，其中政府部門增加 108%



DDoS Attack

新興趨勢：AI技術發展新型態攻擊

- 新型態攻擊與惡意詐騙
  - 113年上半年，AI服務提供商Hugging Face之平台存在惡意AI機器學習模型，其中一些後門更可以讓攻擊者於受害電腦上執行惡意程式
  - 繼112年ChatGPT發生ChatGPT Plus 訂閱者中約有 1.2%(約百萬用戶)資料遭到洩露後，113年上半年再次發生用戶資料及其多個第三方外掛程式中存在洩露，可能遭受零點擊漏洞，意謂不需要求受害者點擊連結或檔案安裝，即可將惡意軟體自動安裝，使攻擊者能夠存取受害者私人 GitHub 儲存庫
- Google Cloud 團隊發表之Cybersecurity Forecast 2024，生成式 AI與大型語言模型 (LLM) 用於網路釣魚、簡訊及其他社交工程攻擊，內容將更加真實且合法，並可大規模操作
- AI技術詐騙案例
  - 113年上半年英國知名跨國工程業者Arup公司，因為深偽技術(Deepfake)，遭受巨額損失，香港分公司員工因虛假之影像與語音向詐騙者支付 2500 萬美元

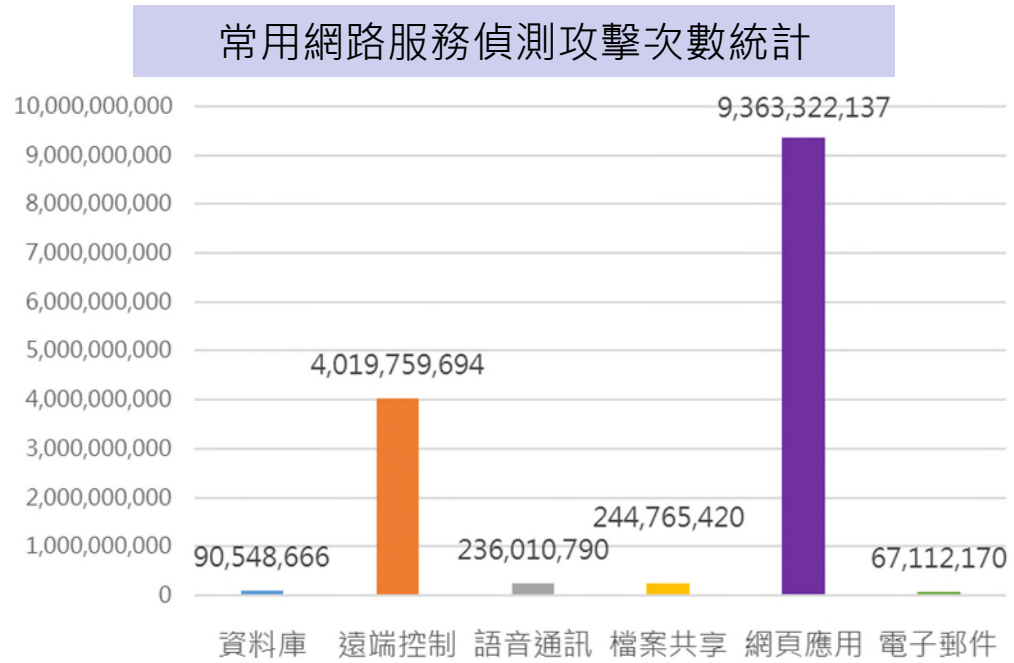


圖片來源: State of Security, The Race to Harness AI, Splunk

政府資通安全威脅趨勢

殭屍網路威脅情蒐(1/2)

- 113年1~9月，透過國內外部署之蜜罐誘捕殭屍網路攻擊威脅，共捕獲18,832,137,012次攻擊連線
  - 前3名攻擊跳板來源國家分別為美國(32%)、俄羅斯(11%)及保加利亞(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
  - 其中捕獲69,794個惡意樣本，以Mirai殭屍網路與其變種最多



殭屍網路威脅情蒐(2/2)

- 113年HailBot與CatDDoS新興之殭屍網路持續針對物聯網進行攻擊
  - 大量利用漏洞感染擴散，主要攻擊目標類型包含路由器、網通設備及DVR監視器等物聯網裝置
  - 殭屍程式以新式加密演算法ChaCha20加密設定檔，以及利用混淆之網路行為規避靜、動態偵測，增加分析之複雜性
    - ChaCha20為對稱加密算法，用於取代RC4之串流加密法
- 因應物聯網殭屍網路之攻擊趨勢，仍需持續宣導物聯網設備之相關威脅風險，提高使用者資安意識，避免設備遭殭屍網路感染

HailBot殭屍網路

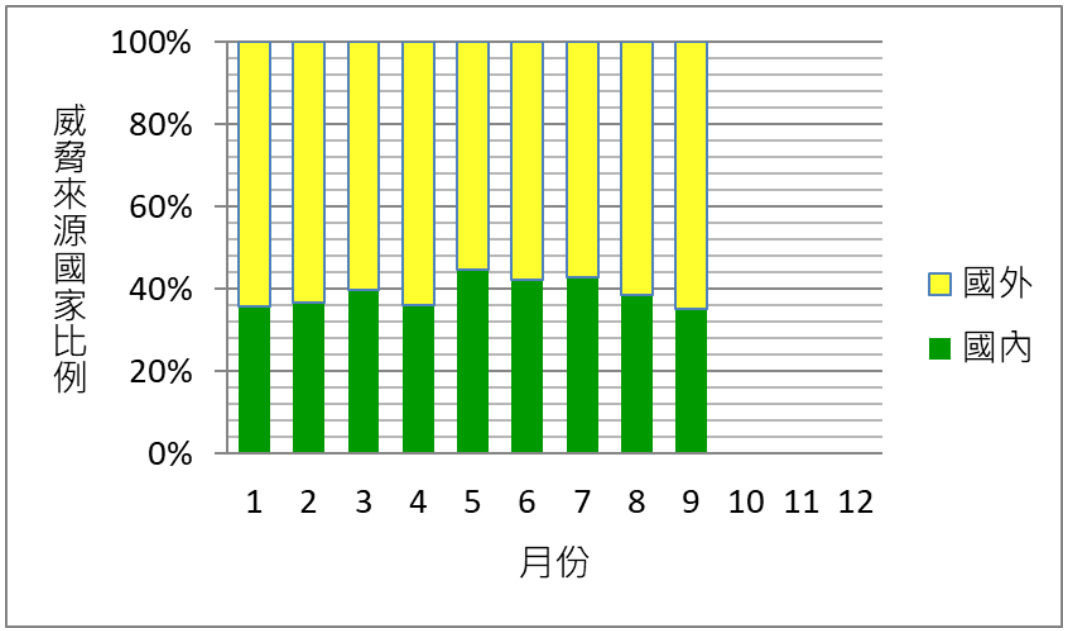
- 113年1~7月發現擴散攻擊活動，攻擊目標包含網通設備、DVR監視器、企業資源計劃系統及數據伺服器
- 感染裝置時具有隱匿惡意檔案與偽裝正常服務之行為

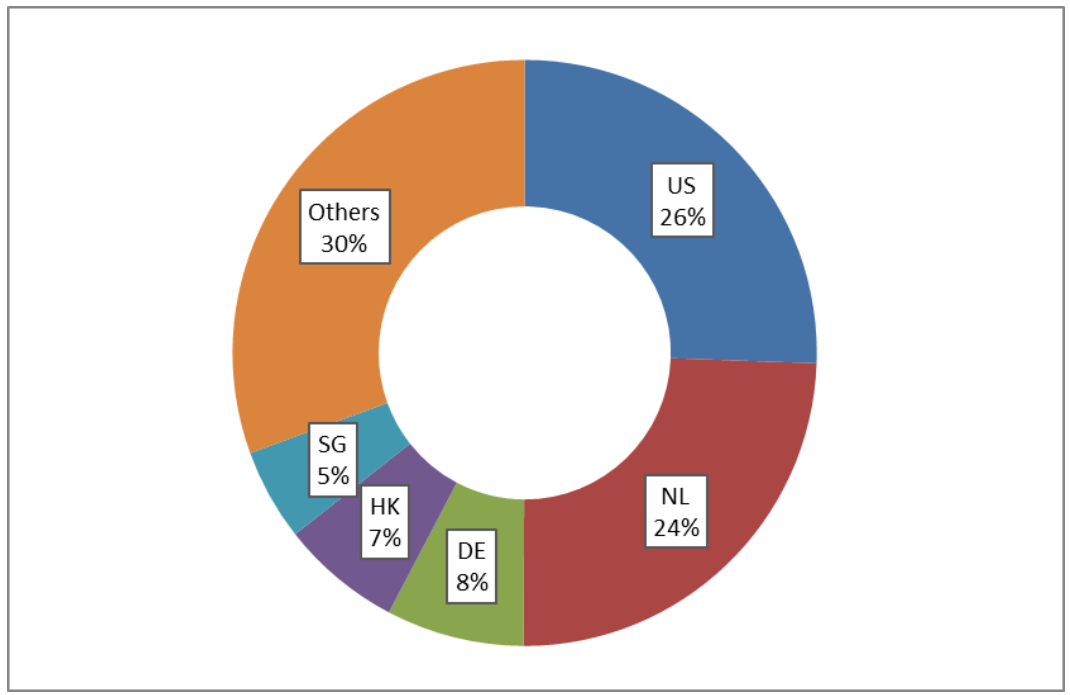
CatDDoS殭屍網路

- 113年5月發現擴散攻擊活動，使用漏洞達16個，攻擊目標包含網通設備、DVR監視器及電信閘道配置管理後台
- 連線至C2報到時，感染裝置回報資訊包含CPU架構類型

聯防監控威脅情蒐(1/3)

- 113年SOC業者回傳有效資安監控情資共655,392件，依政府機關業務類別，前3名分別為綜合行政類之資訊蒐集89,740件、外交國防法務類之資訊蒐集62,186件及外交國防法務類之入侵嘗試29,256件
- 國外攻擊跳板來源前3名分別為美國(26%)、荷蘭(24%)及德國(8%)





聯防監控威脅情蒐(2/3)

- 政府領域網通設備為駭客攻擊目標之一
  - –大華科技物聯網設備漏洞分析
    - ➢該公司生產之物聯網設備於110年6月遭揭露存在身分驗證繞過漏洞，受影響設備包含網路監視器、監視錄影主機、保全門口機及保全室內機等

漏洞編號	CVSSv3分數	漏洞描述
CVE-2021-33044	9.8	不適當的身分驗證
CVE-2021-33045	9.8	不適當的身分驗證

受攻擊機關統計

資安責任等級	B	C	D	總計
受漏洞影響設備數量	30	35	1	66

聯防監控威脅情蒐(3/3)

- 政府領域網通設備為駭客攻擊目標之一
  - –Fortinet網通設備漏洞資安風險分析
    - ➢近期Fortinet公布其所屬產品FortiOS與FortiProxy存在高危風險漏洞

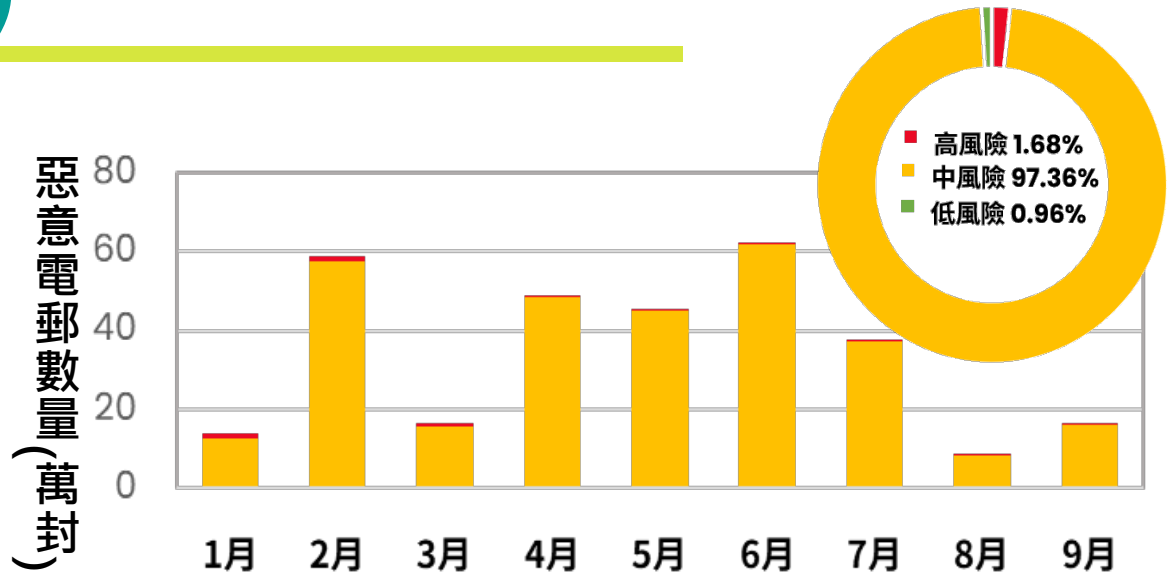
漏洞編號	CVSSv3分數	漏洞描述
CVE-2024-21762	9.6	越界寫入漏洞 (Out-of-Bounds Write)
CVE-2024-23113	9.8	外部控制字串漏洞 (Externally-Controlled Format String)

受攻擊機關統計

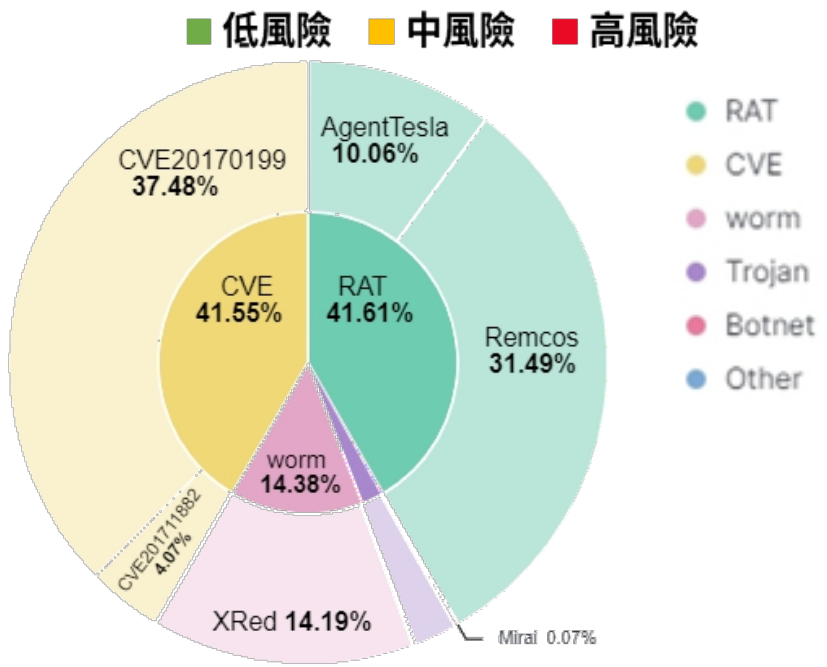
資安責任等級	A	B	C	D	總計
受漏洞影響設備數量	2	11	29	15	57

惡意電子郵件分析(1/2)

- 113年共檢測1.6億餘(166,215,880)封電子郵件，偵測發現**308萬餘(3,080,336)封可疑惡意電子郵件**，占1.85%

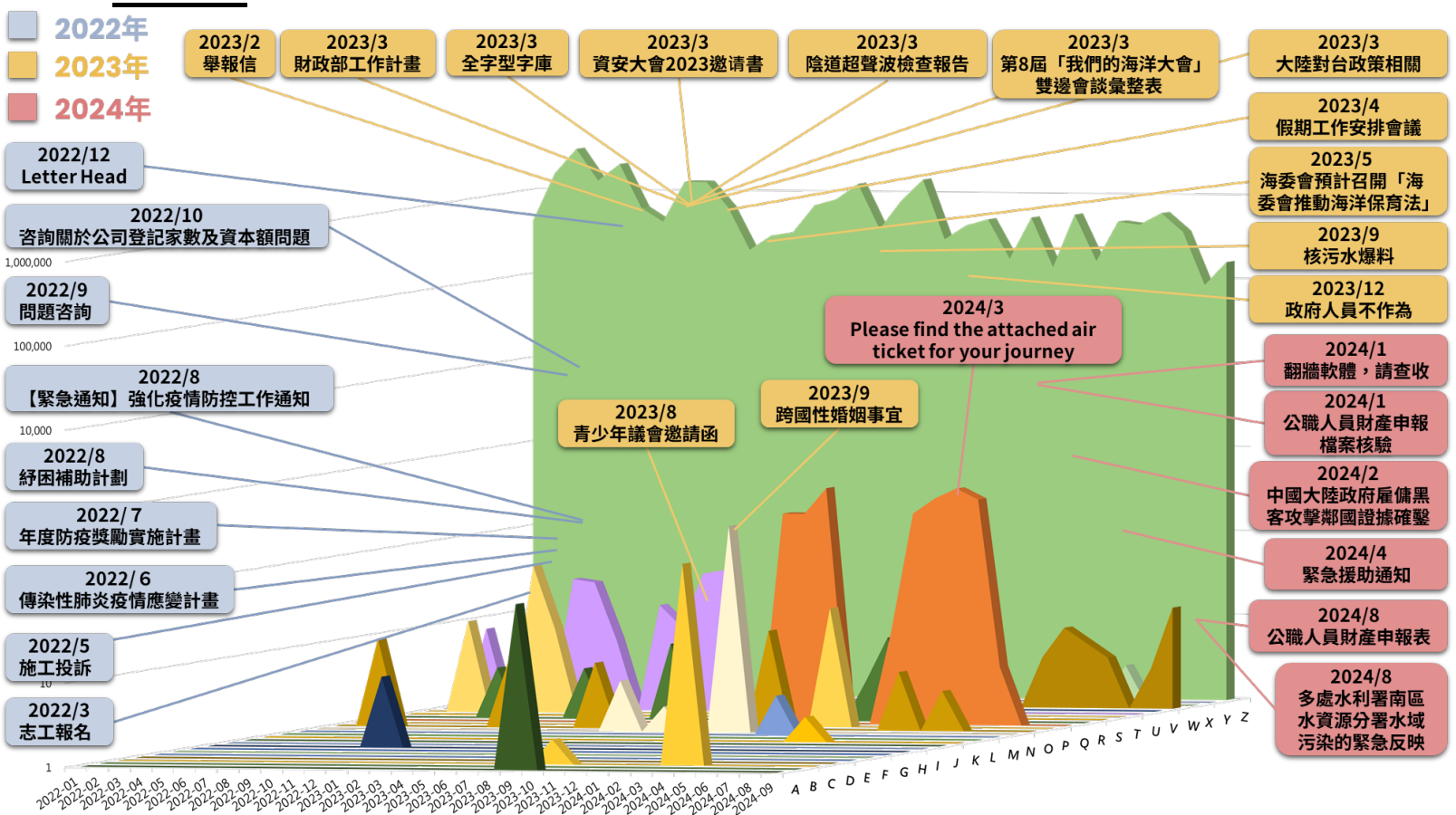


- 含惡意附檔之郵件中，以散布**CVE-2017-0199**漏洞利用之惡意文件最多，其次則為遠端木馬**Remcos**與後門程式**XRed**



惡意電子郵件分析(2/2)

- 113年政府領域APT郵件攻擊趨勢可歸納為**7波攻擊行動**，**計608封針對性社交工程郵件**，駭客利用公職人員財產申報、差旅訂票及檢舉爆料等引誘性主旨，對政府機關人員發動攻擊

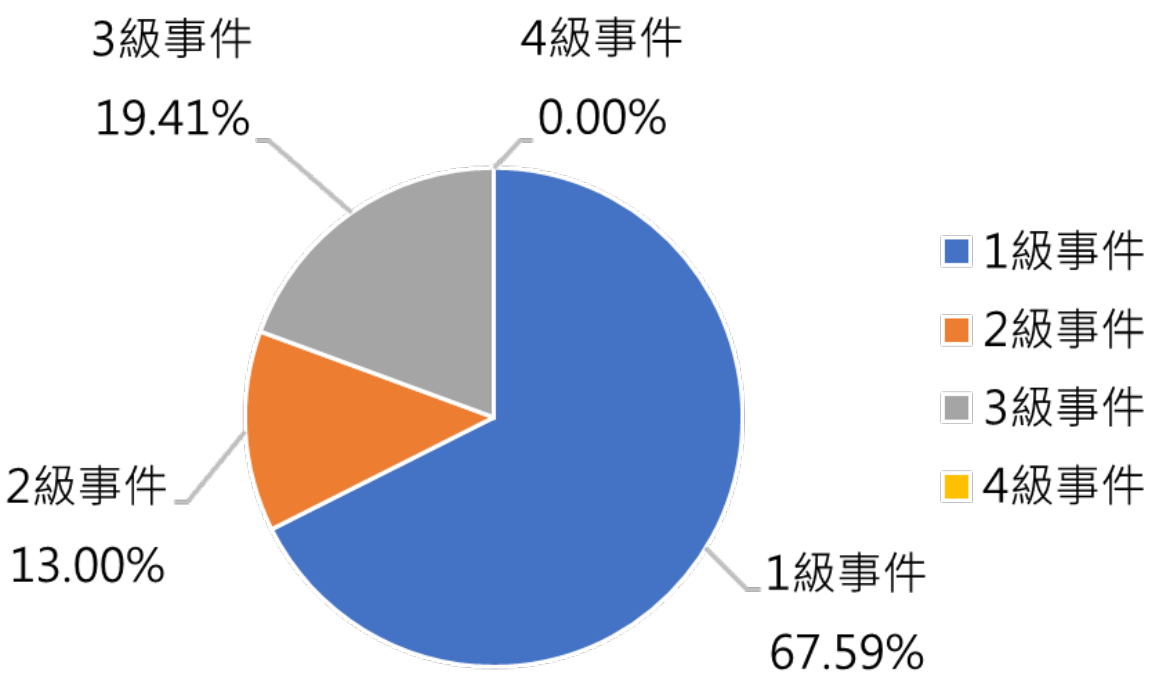


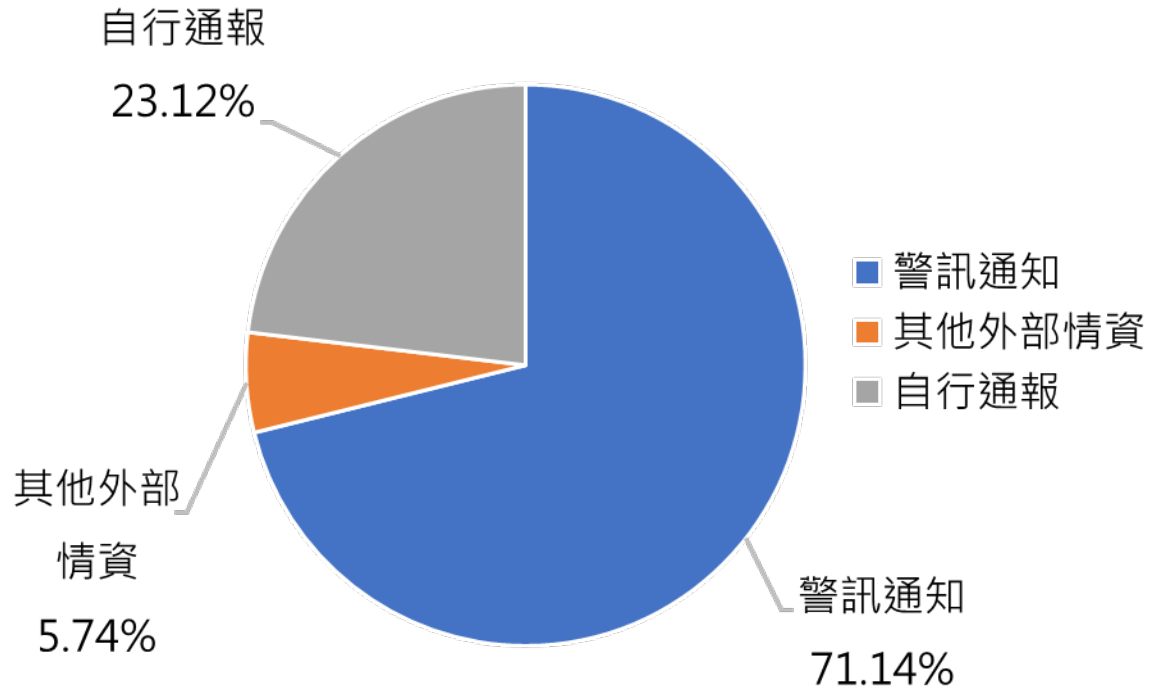
113年APT郵件攻擊手法

- 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
- 以水汙染檢舉為由，利用MSC文件之新型態攻擊手法下載Cobalt Strike後門程式

通報事件分析(1/2)

- 113年1月1日至9月30日共接獲1,185件政府機關資安事件通報
- 事件影響等級以1級事件為主占67.59%
- 71.14%為機關接獲資安院警訊通告後所進行之通報

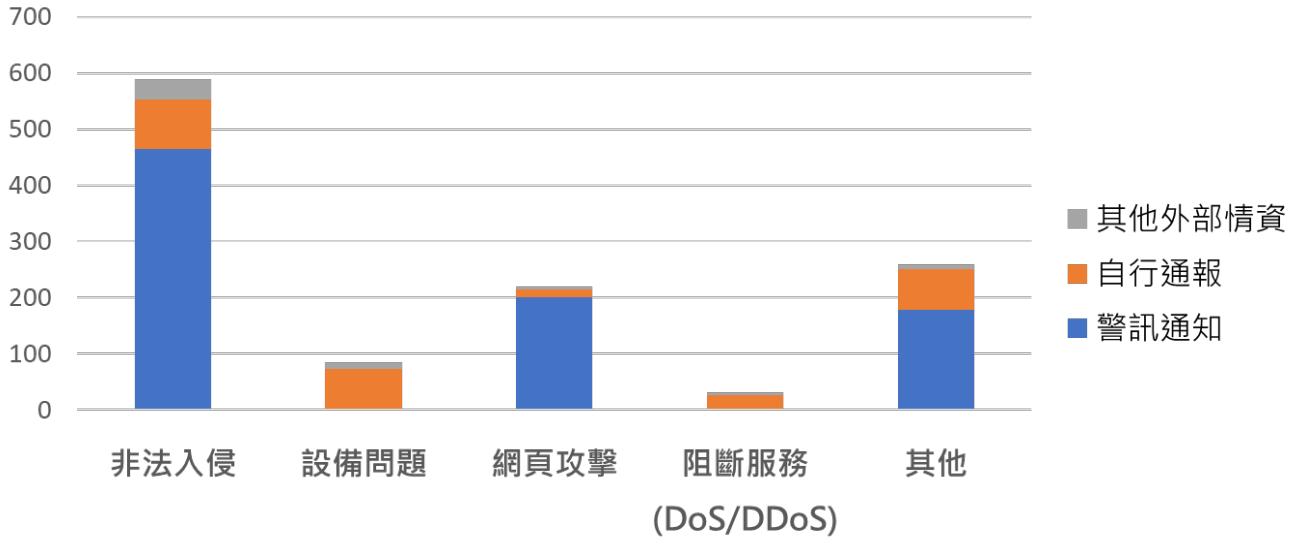




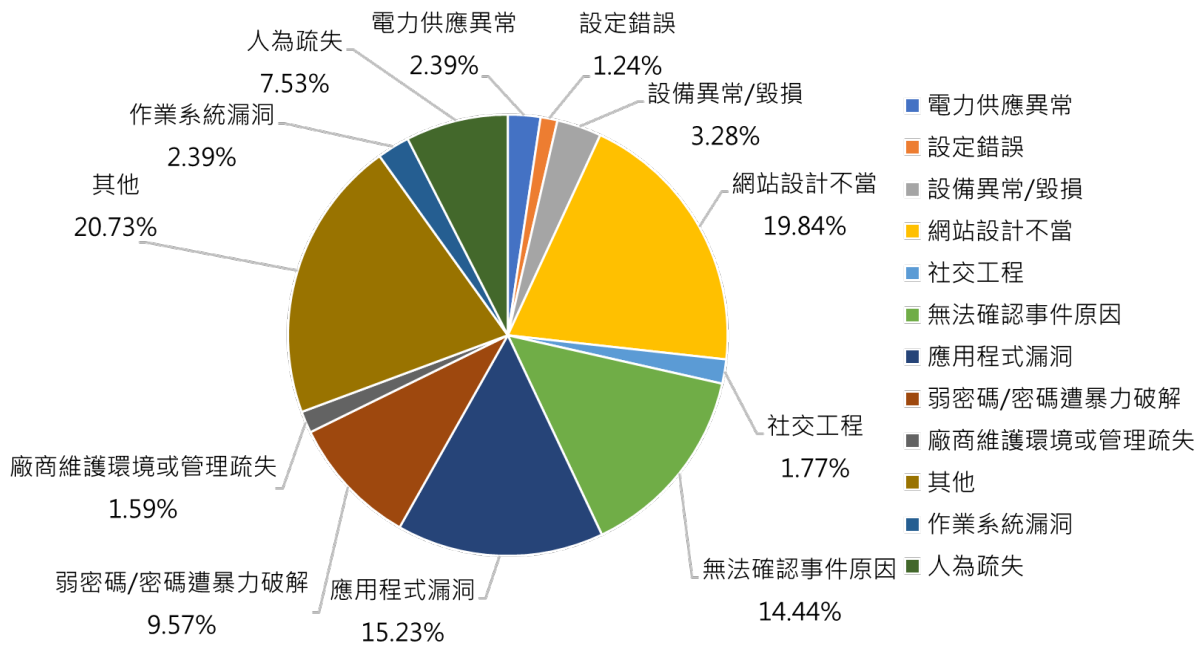
※統計區間：113年1月1日至9月30日

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」 19.84%
  - 「應用程式漏洞」 15.23%
  - 「弱密碼/密碼遭暴力破解」9.57%



※統計區間：113年1月1日至9月30日

政府資安事件案例分析

近期常見資安事件

網通設備疏於更新或使用弱密碼導致存在資安風險

郵件帳號或網站後台**設置弱密碼遭暴力破解**，導致資料外洩

未即時**修補系統漏洞**，導致漏洞遭利用入侵系統

網站遭DDoS攻擊，導致無法正常提供網站服務

人員資安意識不足，開啟惡意郵件或下載夾帶惡意程式之軟體，導致設備受駭

設備與網站資料維護不當，導致系統受駭或資料外洩

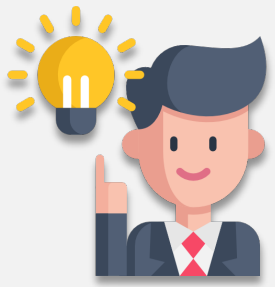
網通設備存在資安風險

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

網通設備疏於更新或使用弱密碼導致存在資安風險

案情提要

- 資安院發現部分機關監視器有殭屍網路Mirai Bot之連線
- 部分機關調查發現監視器存在多項資安風險，包含**多個網路服務暴露於網路**上(如RDP與Telnet等遠端管理通訊協定)、使用**預設密碼/弱密碼**及**韌體版本老舊**



防護建議

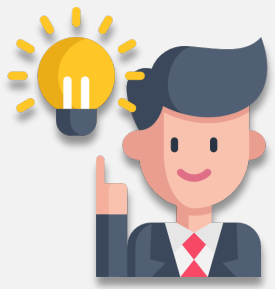
- **關閉不必要的網路服務**
- 使用具**複雜度之密碼**
- 定期檢視並**更新韌體版本**
- 評估汰換或加強防護已停止更新或支援之產品

弱密碼遭破解後惡意利用(1/2)

郵件帳號**密碼提示訊息**暴露過多資訊，使郵件資料存在外洩風險

案情提要

- 部分機關發現電子郵件遭非法轉寄至外部可疑信箱
- 機關調查研判係使用者設定之**密碼提示訊息透漏過多資訊**，導致駭客可透過密碼提示破解密碼登入帳號，修改自動轉寄設定，將電子郵件轉寄至外部可疑信箱



防護建議

- 評估**停用或限制密碼提示功能**，確保提示訊息不包含密碼本身或過多資訊
- 評估啟用**多因子認證或一次性密碼驗證機制**，降低密碼遭暴力破解之風險，並加強異常行為偵測機制，即時監控異常登入與行為

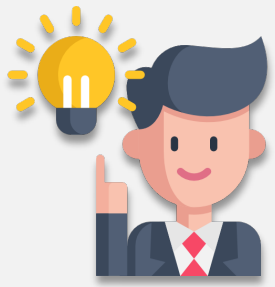
弱密碼遭破解後惡意利用(2/2)

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

粉絲專頁管理者帳號設置弱密碼，遭破解後惡意利用

案情提要

- 某機關發現Facebook粉絲專頁遭駭客盜用，張貼不當圖片
- 機關調查發現**粉絲專頁管理者帳號之密碼設置過於簡單**，遭駭客破解登入後，將其設為管理者並移除其他管理人員



防護建議

- 避免設置常見、與帳號相似或**鍵盤排序等具規則之弱密碼**
- **定期變更密碼**，並且不得與前幾次相同

未即時修補漏洞遭惡意利用(1/3)

駭客利用開源軟體/應用程式漏洞入侵系統

案情提要

案例一

- **PHP程式語言**存在引數注入(Argument Injection)漏洞**(CVE-2024-4577)**，因PHP 程式語言忽略 Windows作業系統內部對字元編碼轉換的Best-Fit特性，導致攻擊者可透過引數注入等攻擊於遠端 PHP 伺服器上**執行任意程式碼**，此漏洞官方已於2024/06/06發佈修復版本
- 部分機關發現網站伺服器遭攻擊，並執行異常指令，經廠商調查，發現駭客皆利用PHP漏洞(CVE-2024-4577)進行攻擊行為

發送特製的請求給php-cgi　**Windows的Best-Fit特性會讓CGI程序把0xAD轉換為字元“-”**

POST /**php-cgi/php-cgi.exe**?%ADd+cgi.force_redirect%3D0+%ADd+cgi.redirect_status_env+%ADd+allow_url_include%3D1+%ADd+auto_prepend_file%3Dphp://input

於Access Log中，發現漏洞CVE-2024-4577攻擊語法

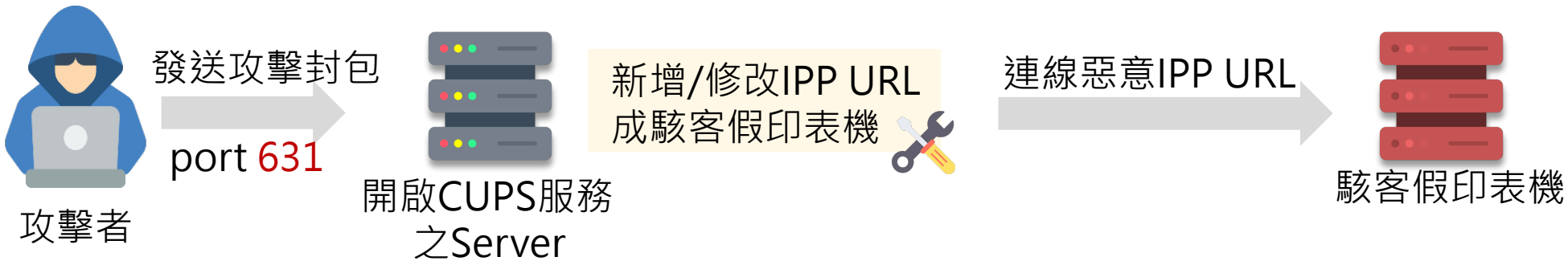
未即時修補漏洞遭惡意利用(2/3)

駭客利用開源軟體/應用程式漏洞入侵系統

案情提要

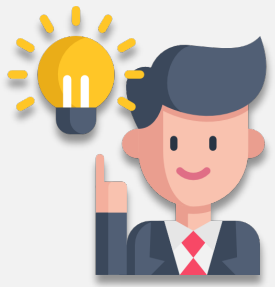
案例二

- **Unix通用列印系統(Common UNIX Printing System，CUPS)**主要透過網路列印協定(IPP)來管理和處理列印任務，近期被發現存在一系列安全漏洞(**CVE-2024-47076、CVE-2024-47175、CVE-2024-47176及CVE-2024-47177**)，未經身分鑑別之遠端攻擊者，有機會可利用漏洞於受影響之Unix作業系統執行任意程式碼
- 資安院發現部分政府機關資訊設備CUPS服務遭利用產生對外連線



未即時修補漏洞遭惡意利用(3/3)

駭客利用開源軟體/應用程式漏洞入侵系統



防護建議

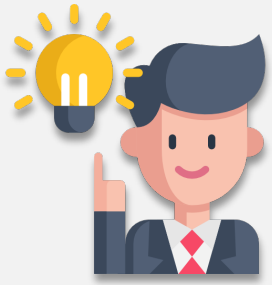
- 應盤點與注意網站使用的套件或軟體，並透過定期檢視與弱點掃描等安全性檢測，掌握系統版本更新與安全狀態，**及時完成漏洞修補作業**
- 若因故無法及時修補漏洞(如原廠尚未釋出更新版)，應即**採取相關防護措施**，降低弱點遭利用導致網站遭入侵的風險

網站遭阻斷服務攻擊

網站遭阻斷服務攻擊，影響系統服務

案情提要

- 部分機關發現官網服務緩慢或中斷，調查發現網站被大量國外IP進行**阻斷服務攻擊**，進而影響系統服務
- 攻擊手法包含
  - HTTPS Flood
  - SYN Flood



防護建議

- 採購**流量清洗**服務
- 限制查詢次數
- 啟用基於行為的**防禦機制**，檢測流量異常

人員資安意識不足(1/7)

至非官方網站下載軟體或下載破解版工具，載到夾載惡意程式之軟體

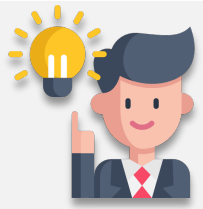
案情提要

案例一

- 資安院發現某機關資訊設備有**竊資軟體**特徵之連線
- 機關調查發現係同仁於google搜尋**winrar破解程式**，並從搜尋結果中下載並執行了惡意程式，導致電腦受駭

案例二

- 資安院發現某機關資訊設備連線惡意中繼站
- 機關調查發現係同仁至連線設備於**非官方網站**下載影音軟體，於軟體安裝過程中，惡意程式亦一併遭安裝至電腦，導致電腦受駭



防護建議

- 機關應建立內部軟體下載與安裝相關規範
- 要求人員**不應於公務設備安裝非公務使用軟體**，如因業務需求須安裝軟體，應至**官方網站下載並安裝**

人員資安意識不足(2/7)

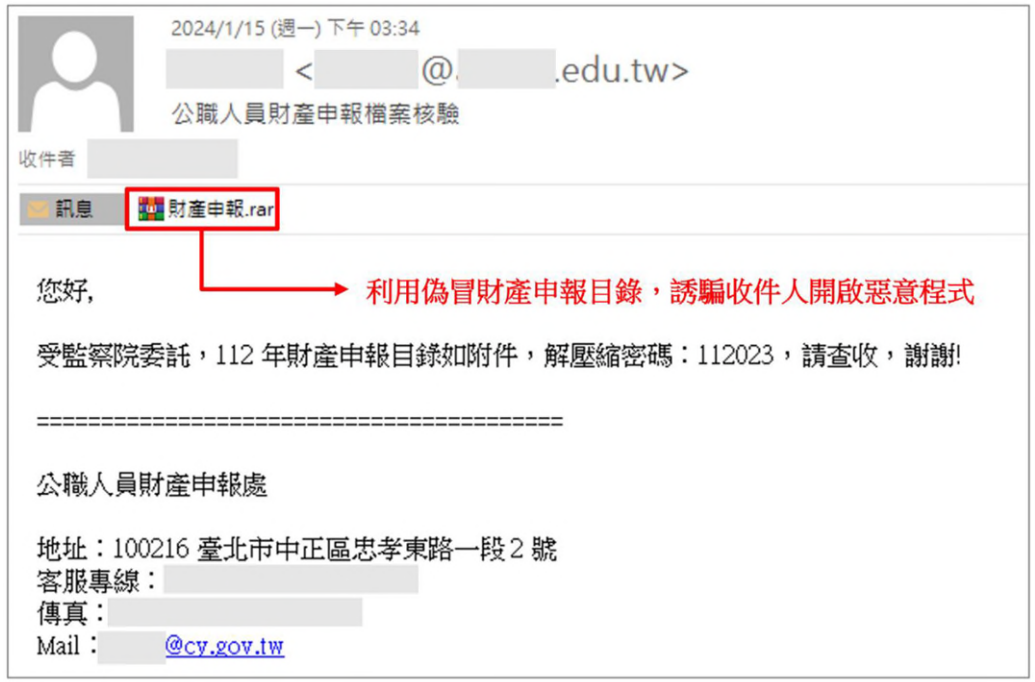
國家資通安全研究院
National Institute of Cyber Security

點擊社交工程郵件內的連結或附件，導致電腦受駭或資料外洩

案情提要

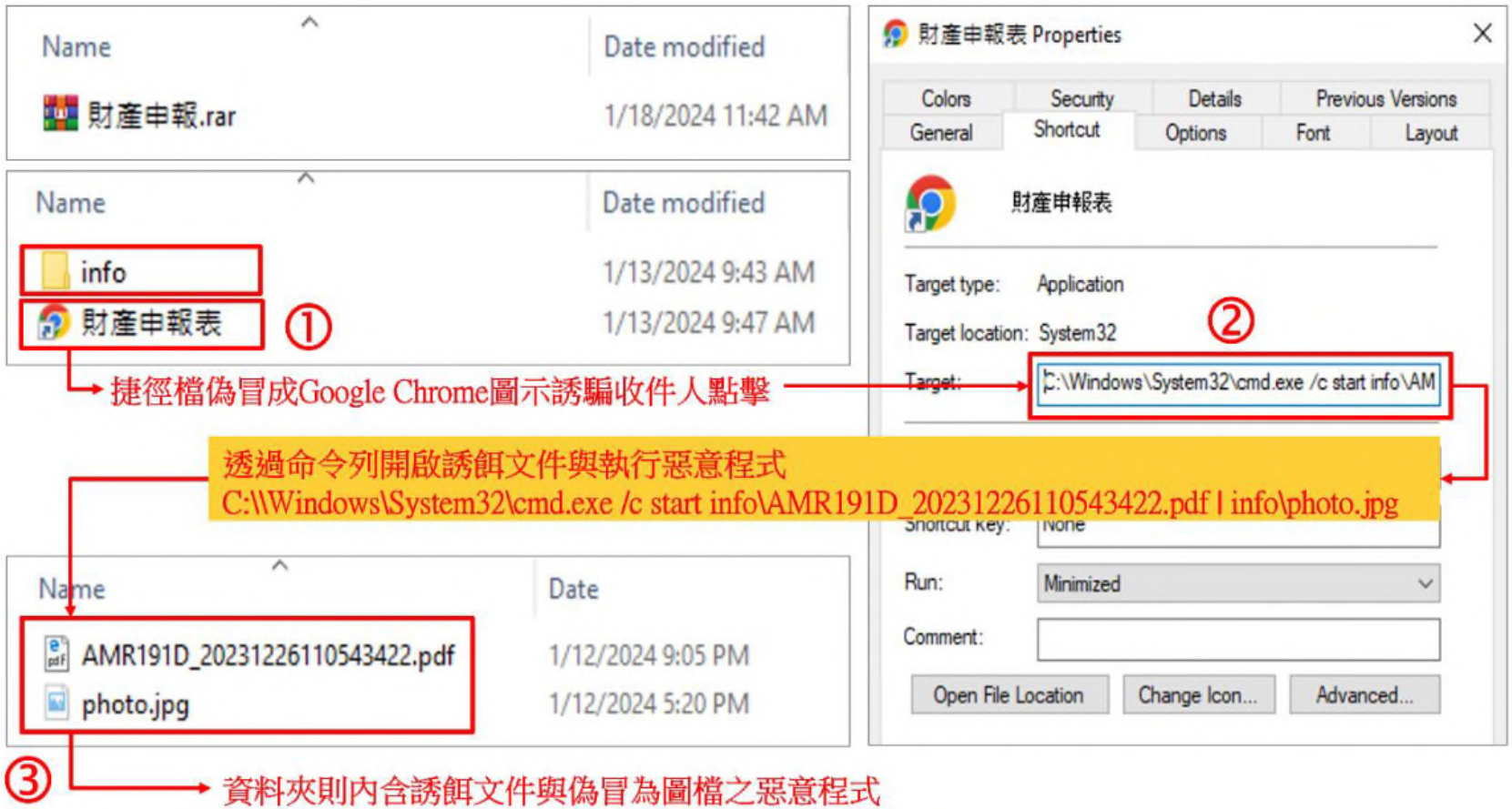
案例一

- 資安院發現駭客利用大學系所人員之電子郵件帳號，偽冒監察院名義，**寄送含惡意附檔之社交工程電子郵件**給政府機關人員
- 信件主旨：公職人員財產申報檔案核驗
- 部分政府機關人員接獲信件後，信以為真，啟惡意附檔後遭植入後門程式



人員資安意識不足(3/7)

點擊社交工程郵件內的連結或附件，導致電腦受駭或資料外洩



- 若收件人點擊該捷徑檔，將執行惡意程式與開啟誘餌文件，且惡意程式會建立常駐機制並**連線至惡意中繼站**
- 惡意程式為 Star RAT 變種惡意程式，駭客可透過惡意程式對主機進行文件管理、鍵盤側錄、系統管理、螢幕控制、語音監聽及執行遠端命令等功能

人員資安意識不足(4/7)

點擊社交工程郵件內的連結或附件，導致電腦受駭或資料外洩

案情提要

案例二

- 資安院發現駭客使用ProtonMail免費郵件服務帳號，以反映**水域汙染議題名義**，並假造公害污染**陳情文件**之惡意檔案，對特定機關業務窗口發動魚叉式社交工程攻擊，透過公務相關主旨誘騙目標收件人開啟惡意檔案
- 收件人執行附件檔案，會下載並載入惡意 DLL 檔，接續惡意 DLL 檔會下載惡意Shellcode檔案並連線至第一個惡意中繼站，且部署Cobalt Strike後門程式後，最終**連線至 Cobalt Strike 惡意中繼站**

人員資安意識不足(5/7)

點擊社交工程郵件內的連結或附件，導致電腦受駭或資料外洩

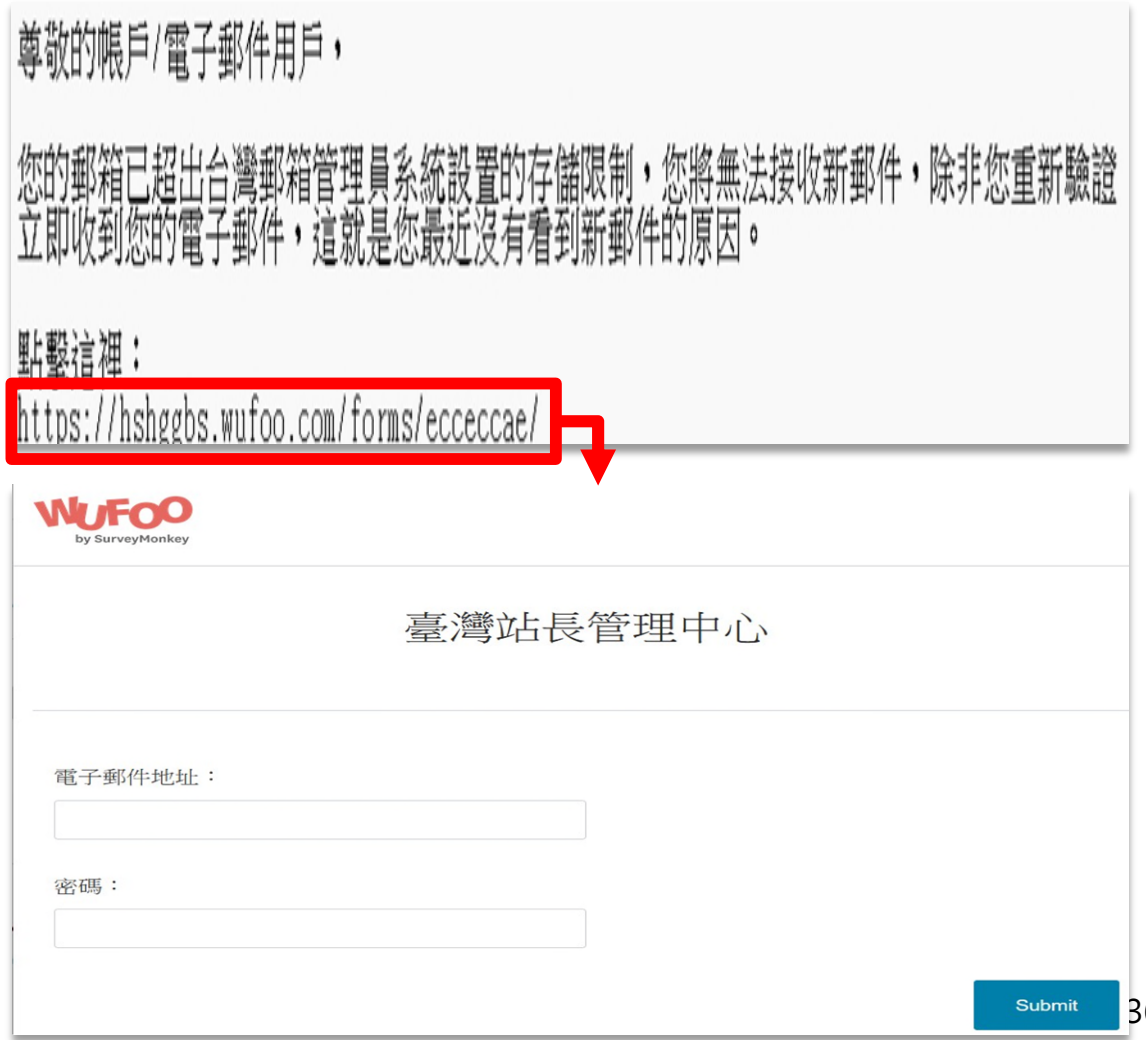
人員資安意識不足(6/7)

點擊社交工程郵件內的連結或附件，導致電腦受駭或資料外洩

案情提要

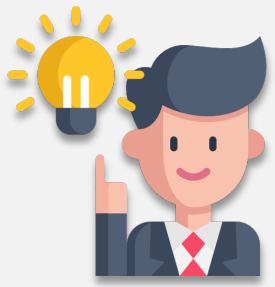
案例三

- 某機關發現多名同仁信箱遭盜用**對外發送惡意郵件**
- 調查發現多名同仁接獲社交工程郵件，部分同仁遭誘騙**點擊連結並登打帳密資料**，導致郵件帳密外洩並遭駭客利用對外發送惡意郵件



人員資安意識不足(7/7)

點擊社交工程郵件內的連結或附件，導致電腦受駭或資料外洩



防護建議

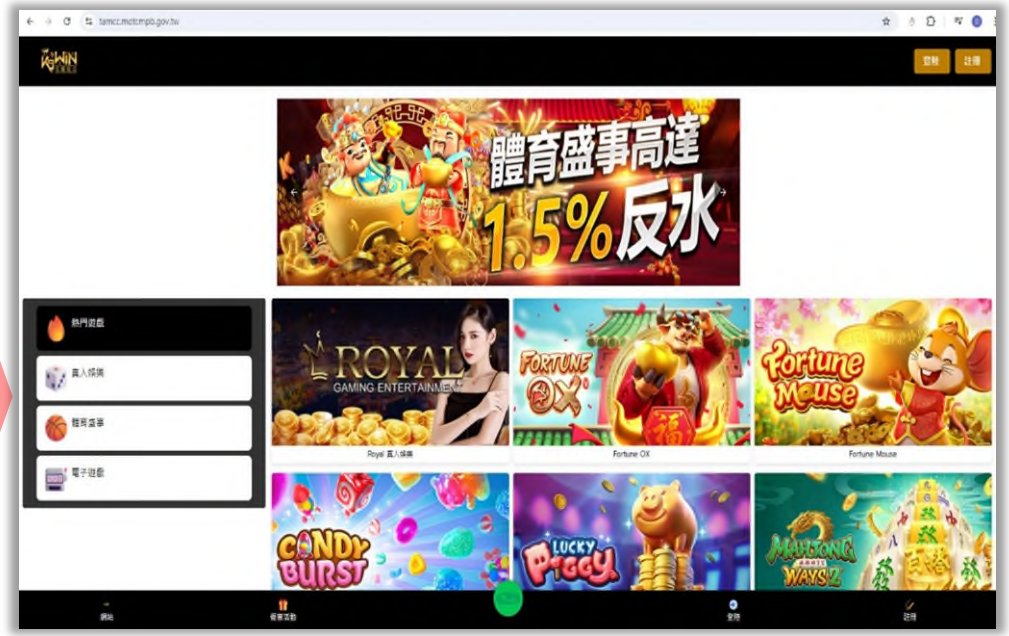
- 承辦人員與業務窗口應留意業務相關主旨之可疑電子郵件，注意**郵件來源正確性，勿開啟不明來源之郵件與相關附檔及連結**
- 加強內部宣導，提升人員資安意識
- 確認電子郵件附檔屬性或檔名後才點擊檔案，若發現檔案名稱中存在**異常字元**(如 pdf.zip, pdf.exe, lnk, rcs, exe, moc 等可執行檔案副檔名或相關之逆排序，以及檔名為亂碼或簡體字等)，請提高警覺

設備與網站資料維護不當(1/4)

未妥善管理子域名，導致遭重定向至不當網站

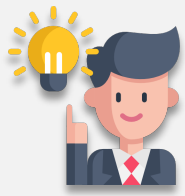
案情提要

- 部分政府機關舉辦之活動或對外服務網站，由於**未妥善管理子域名**，導致**DNS CNAME**劫持事件發生，有心人事藉此將網頁重定向至不當網站



設備與網站資料維護不當(2/4)

未妥善管理子域名，導致遭重定向至不當網站



防護建議

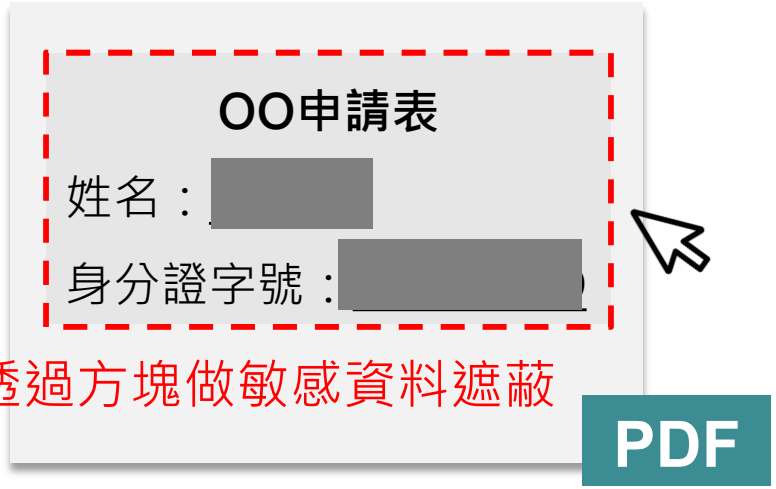
- 機關應掌握所核發之子網域使用情況
- 定期**檢視DNS紀錄**，**移除不再使用之CNAME紀錄**，並確保外部服務停止時及時更新或刪除紀錄

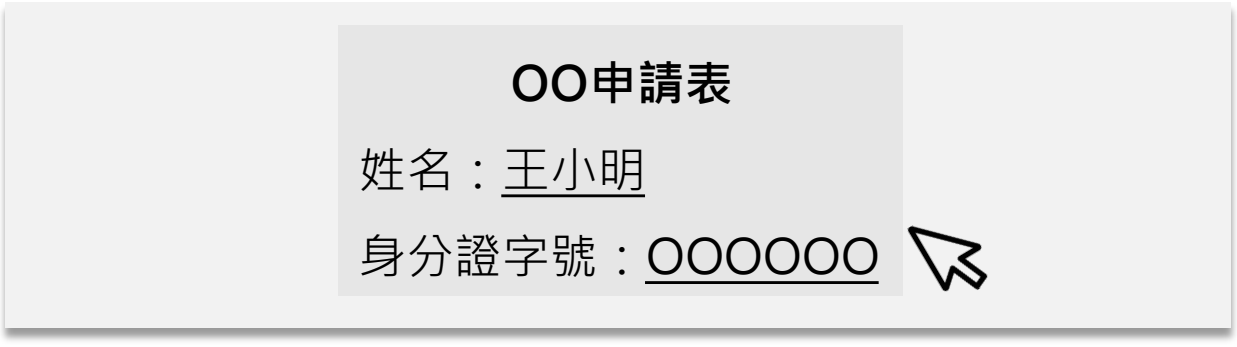
設備與網站資料維護不當(3/4)

公開文件中敏感資料未有效遮蔽，使敏感資料存在外洩之風險

案情提要

- 機關為方便民眾操作網站服務，提供說明文件檢附實際申請書或操作畫面範例
- 部分文件圖片之敏感資料遮蔽處理，僅於圖片加上黑色方塊或其他圖層，底層之完整圖片資料仍保留於文件中，有心人士可透過**Adobe Reader複製底層圖片並存放於其他文件**，進而檢視被遮蔽內容，使敏感資料存在外洩之風險

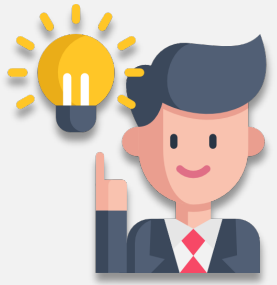




使用**Adobe Reader開啟檔案**，右鍵複製底層圖片，並於其他文件貼上，即可檢視敏感資料內容

設備與網站資料維護不當(4/4)

公開文件中**敏感資料未有效遮蔽**，使敏感資料存在外洩之風險



防護建議

- 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
- 在公開涉及個人資料文件前，應進行全面檢視，**確保個人資料已移除或經適當遮蔽處理**
- 應定期進行資安教育訓練，提升內部人員對個人資料保護之認識及熟悉正確資料遮蔽處理流程

「個人資料保護法」第 12 條

公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人

政府機關資安防護強化重點

強化網通設備安全與防護整備
落實資安防護監控降低更新延遲風險
落實資通訊系統/服務維護管理

強化網通設備安全與防護整備

加強網通設備存取控管

- 評估開放外部存取之必要性，若有對外開放之需求，應確保僅**開放必要服務**
- 避免使用預設密碼或常見密碼，設置具**強韌性的密碼**並定期更換

及時更新軟體與韌體版本

- 留意所採購產品之**版本更新情形**，以及時修補漏洞，降低遭入侵之風險
- 若產品已釋出停止支援更新訊息，應儘早評估汰換或採取相關因應措施

確認日誌記錄功能

- 確認設備可使用之**日誌記錄功能**與保存項目
- 評估日誌可保存期限並落實儲存

落實資安防護監控降低更新延遲風險

透過定期檢視與弱點掃描等安全性檢測，掌握各系統版本更新與安全狀態，及時完成漏洞修補作業，若因故無法及時修補漏洞(如原廠尚未釋出更新版或系統相容性問題)，應即採取**相關防護措施**或**加強資安防護監控**，降低弱點遭利用之風險

採取緩解措施

- 加強**存取控管**(如白名單限制存取)
- 採用官方建議的**緩解方法**
  (如調整設定或限制某些功能的使用)

加強監控

- 加強**漏洞利用**的防護監控
- 監控系統或服務之**異常行為**

落實資通訊系統/服務維護管理

政府機關執行短期業務或辦理活動，常委請廠商建置網站以宣導或發布活動相關訊息，惟業務或活動結束後，網站因**疏於維護管理**導致存在資安風險，如遭惡意置換，為避免這些風險，建議落實相關的網站管理與安全措施

建立管理程序

- 訂定並**落實網站上/下線相關作業程序**
- 若網站已無使用需求，應及時**撤銷域名**並**下架網頁**，避免衍生資安疑慮

稽查使用情形

- 定期稽查對外服務網站**使用情形**
- 新舊系統併行期間，**舊系統亦應做好資安防護**，依機關規定時程進行系統更新與弱點掃描等防護措施

結論與建議(1/2)

- 針對的**網通設備**攻擊事件(如路由器、防火牆及物聯網設備)日益增加，建議各機關關注相關漏洞情資，提升弱點防護能力，並落實資安監控措施
  - 關注**漏洞情資**：包括網通設備漏洞資訊與零日攻擊等，並適時更新軟體或韌體版本，採取相關防護設定以降低資安風險
  - 落實資安防護措施：確保網通設備不使用預設密碼或弱密碼，並避免暴露過多服務於網路上(如 RDP與Telnet 等遠端管理通訊協定)。應設定強健的密碼，並**僅開放必要服務**以降低受攻擊之風險
- 落實資通訊系統/服務維護管理
  - 應訂定並**落實網站上/下線相關作業程序**，及時下架已無使用需求之網站，並撤銷域名

結論與建議(2/2)

- 強化內部人員對資通安全與**敏感資料保護**意識
  - 避免於公務電腦上安裝非公務用途軟體
  - 注意郵件來源正確性，慎防異常附件與連結
  - 落實個資「認知宣導及教育訓練」，公開涉及個人資料文件前，應確保個人資料**已移除或經適當遮蔽處理**
- 落實資安防護監控**降低更新延遲風險**
  - 掌握各系統版本更新與安全狀態，以及時完成漏洞修補作業
  - 若因故無法及時修補漏洞，應即**採取相關防護措施**或加強資安防護監控，降低弱點遭利用之風險

報告完畢
敬請指教