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

大綱

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

- 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
- 強化政府數位韌性
- 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

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

- 綜整2023年全球資安威脅報告，歸納資安威脅趨勢分為六大類，對應網際攻擊狙殺鍊(Cyber Kill Chain)如下

偵查、武裝、遞送

個人資料與憑證外洩致防護機制失效

資通系統弱點頻遭揭露利用

雲端應用服務衍生多元威脅

資安(訊)供應商駭侵破壞邊界防護

攻擊、安裝

社交工程泛濫致APT鎖定與勒索軟體風險增加

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

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

- IBM 2023年資料外洩成本報告(Cost of a Data Breach Report 2023)調查顯示，資料外洩於2023年平均成本高達445萬美元，相較2022年增加2.3%，資料外洩平均成本呈現年年增長趨勢
  - 資料外洩成本首位為美國$9.48(百萬)、第2名為中東國家$8.07(百萬)，第3名為加拿大$5.13(百萬)，亞洲國家包含(第 5 名)日本$4.52(百萬)、南韓(第10名)$3.48(百萬)

2023.11.28 | 資訊安全

LINE母公司遭駭，超過40萬筆個資外洩、台灣也遭殃！背後原因跟Naver有關？

《日經新聞》在今日率先報導指出，日本LINE雅虎公司宣布伺服器遭到網路攻擊，追溯整起遭駭原因，與最大股東Naver有關。

#資訊安全 #駭客攻擊

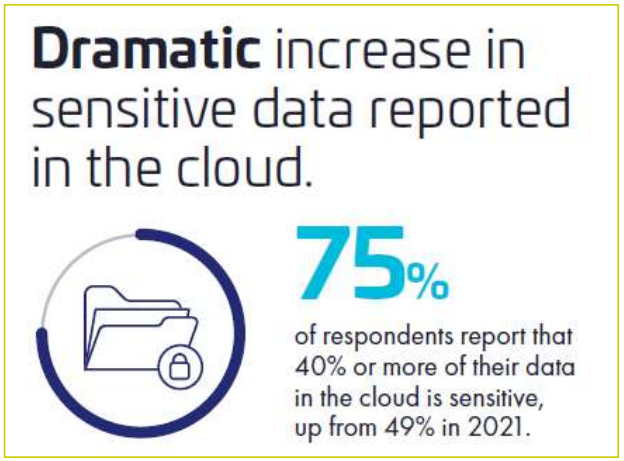
圖片來源：https://www.bnext.com.tw/article/77571/line-japan-hack-naver?

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

雲端應用服務衍生多元威脅

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

- 資安廠商Thales 2023年雲端安全研究報告指出，組織面對多個雲端服務供應商已成為未來趨勢
- 2023年超過3/4受訪者表示有2個以上之雲端服務供應商，至於是否會將機敏資訊放置於雲端，2021年只有49%受訪者會將機敏資訊放置於雲端，2023年有75%受訪者表示會如此做，且放置於雲端機敏資訊平均約占40%
- 雖然使用者逐漸習慣放置機敏資訊於雲端，惟平均只有45%機敏資料會被加密
- 人為錯誤是雲端資料外洩之主要肇因，超過五成之受訪者表示因為雲端架構複雜，雲端管理與操作資料不易，因此造成資料外洩



圖片來源:
https://cpl.thalesgroup.com/cloud-security-research#download-popup

社交工程泛濫致APT與勒索風險增加

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

- Google 2024年網路安全預測，運用生成式AI與LLMs將可使網路釣魚活動更加專業化，藉由智慧與巨量資料衍生之攻擊手法與策略，如將以往可能會出現之拼字或語法措辭，修飾為更加與原有時事、流程及版本相似，且客製化讓人信服之假冒合法或擬真訊息，如此一來將可對鎖定目標對象展開精準攻擊
- 駭客使用動態策略擴散攻勢，經常變更主機名稱、路徑、檔名或多種結合時事等元素擴散勒索軟體，過去電子郵件附件是主要傳播工具，隨著社群媒體盛行，現行主要傳播方式已變更為透過URL連結與網頁瀏覽，約占勒索軟體案例七成以上

圖片來源:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

資通系統弱點頻遭揭露利用

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

- 資安廠商Qualys公布2023年前十大被利用之漏洞
  - SugarCRM遠端程式碼執行(RCE)漏洞
  - VMware Aria Operations for Networks指令注入漏洞
  - Barracuda電子郵件安全閘道漏洞
  - Windows共通日誌檔案系統驅動程式權限提升漏洞
  - 3CX桌面用戶端供應鏈漏洞
  - MOVEit傳輸注入漏洞
  - Microsoft Outlook提權漏洞
  - Fortra GoAnywhere託管檔案傳輸(Managed File Transfer, MFT)之遠端程式碼執行(Remote Code Execution, RCE)漏洞
  - Windows SmartScreen安全功能繞道漏洞
  - PaperCut NG/MF多個安全漏洞

關注事項
- **漏洞存在時間**
- **修補率**

資安(訊)供應商遭駭破壞邊界防護

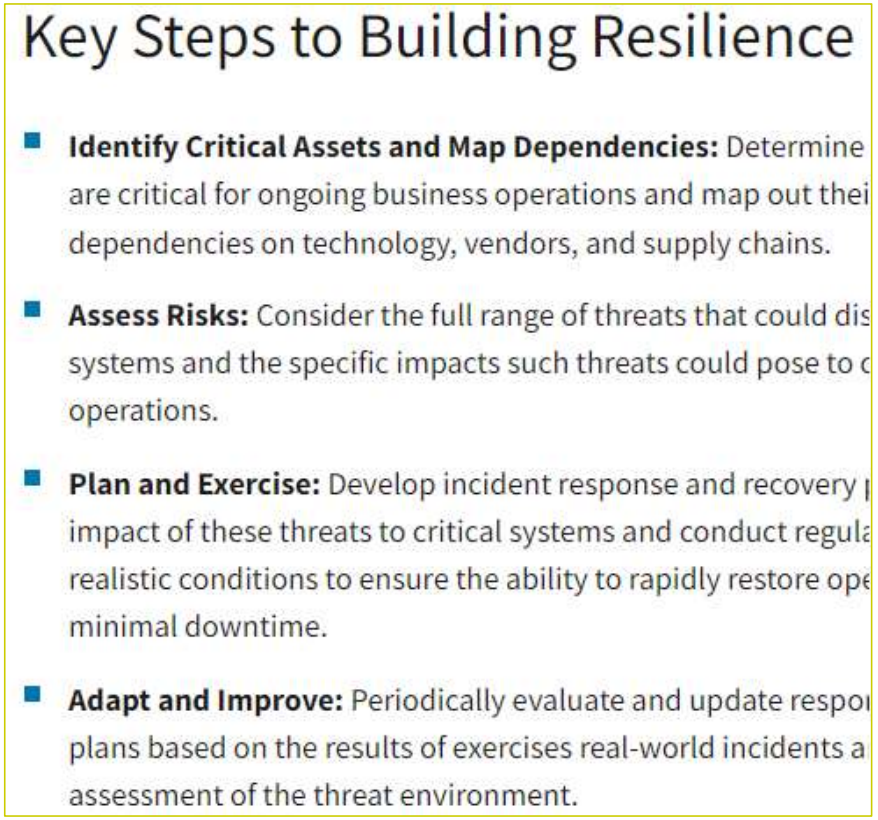
國家資通安全研究院
National Institute of Cyber Security

- Gartner預測2025年全球約有45%組織會因軟體供應鏈遭攻擊，相較於2021年，約是3倍成長率
- 網路安全廠商Cybersecurity Ventures發表軟體供應鏈入侵報告(2023 Software Supply Chain Attack Report)，預測至2031年全球因軟體鏈攻擊事件對組織所造成之損失將高至1,380億美元
- 社交工程與網路釣魚則是最常見入侵之手法
- 其他軟體供應鏈可能發生之威脅路徑
  - 藉由竊取憑證
  - 入侵開發流程之持續整合與持續交付 (Continuous Integration/Continuous Delivery, CI/CD)
  - 系統漏洞或開源軟體之元件
  - 偽冒網域名稱
  - 內部人員威脅

關鍵資訊基礎設施與OT攻擊面向增加

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

- 工業網路社群(Industrial Cyber Community)論壇指出，2023年針對美國關鍵基礎設施所發動之網路威脅激增，特別是針對醫療健康與供水之標的
- 美國國土安全部(DHS)、網路安全與基礎設施安全局(CISA)及聯邦緊急事務管理局(FEMA)等，因洞見關鍵基礎設施之威脅，公布發展盾牌就緒(Shields Ready)行動，藉以激勵關鍵基礎設施所有利害關係者提出具體防禦計畫之時程，以減緩特定威脅之風險



Key Steps to Building Resilience

- **Identify Critical Assets and Map Dependencies:** Determine
  are critical for ongoing business operations and map out thei
  dependencies on technology, vendors, and supply chains.
- **Assess Risks:** Consider the full range of threats that could dis
  systems and the specific impacts such threats could pose to c
  operations.
- **Plan and Exercise:** Develop incident response and recovery
  impact of these threats to critical systems and conduct regula
  realistic conditions to ensure the ability to rapidly restore ope
  minimal downtime.
- **Adapt and Improve:** Periodically evaluate and update respo
  plans based on the results of exercises real-world incidents a
  assessment of the threat environment.

資料來源:https://www.cisa.gov/shields-ready

新興威脅趨勢：生成式AI

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

- 根據AI 廠商Portal 26發表State of Generative AI 2023年報告指出，高達73%受訪者表示曾發生生成式AI技術遭濫用之事件，85%受訪者主要憂慮隱私與安全之風險
- 生成式AI內容農場，相關技術已能利用自動化且以更具效率方式產生不實內容
  - 網站(CelebritiesDeaths.com)為專門刊登名人過世消息之平台，於112年刊載由AI生成之文章，標題即為美國總統拜登逝世、副總統賀錦麗將出任代理總統
  - 內容農場製造之假訊息亦會藉由偽冒貌似新聞網站增加其可信度
- 網路安全廠商Perception Point 2024年報告，2023年社交工程發動之商業電子郵件詐騙事件，相較於2022年只有1 %運用生成式AI技術，2023年躍升至18.6%
- Osterman Research 2023年報告(The Role of AI in Email Security: Exclusive Report by Osterman Research)統計數據，網路犯罪正快速運用AI科技，有超過9成以上之組織接收過生成式AI產生之電子郵件

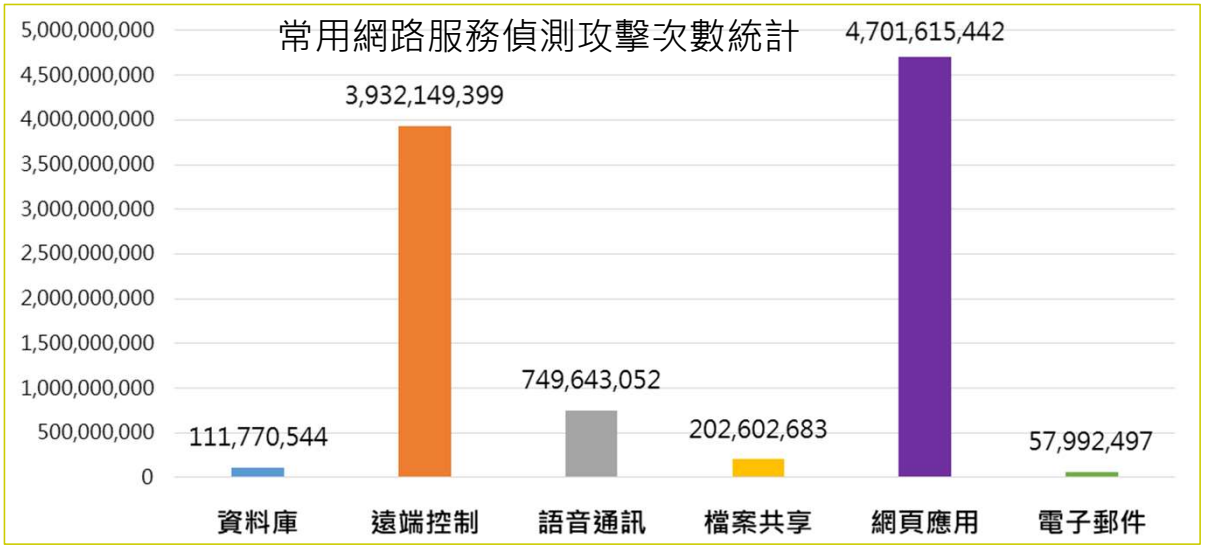
國家資通安全研究院
National Institute of Cyber Security

政府資通安全威脅趨勢

殭屍網路威脅情蒐(1/2)

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

- 112年透過國內外部署之蜜罐誘捕殭屍網路攻擊威脅，共捕獲14,213,863,692次攻擊連線
  - 前3名攻擊跳板來源國家分別為美國(33%)、中國(9%)及新加坡(7%)
  - 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26,546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)

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

- 112年Mirai變種與其他新興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、網通設備及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變種

- 變種持續增加，頻繁更新擴散使用之CVE漏洞
- 「most」變種即使用113年初揭漏之CVE-2024-0778攻擊Uniview(宇視)監控錄影主機，其C2伺服器位於越南

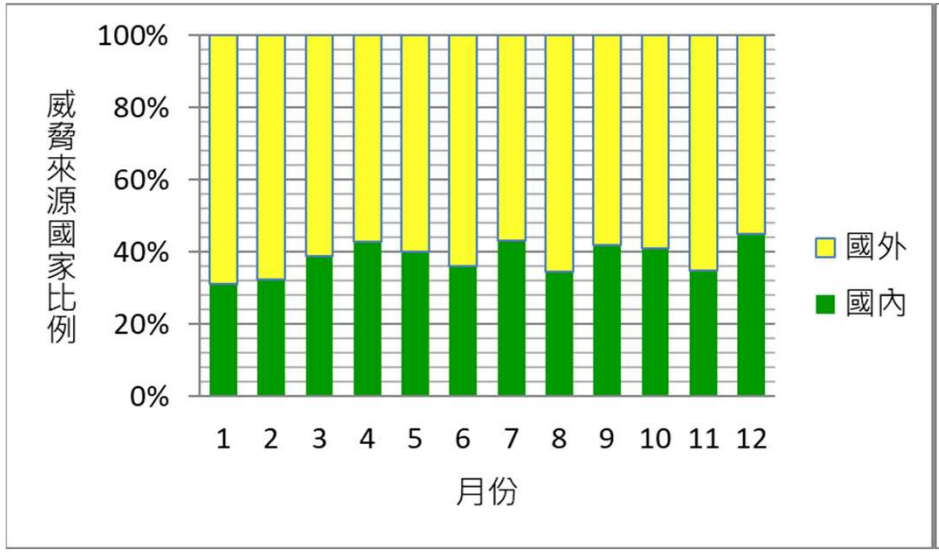
Zerobot殭屍網路

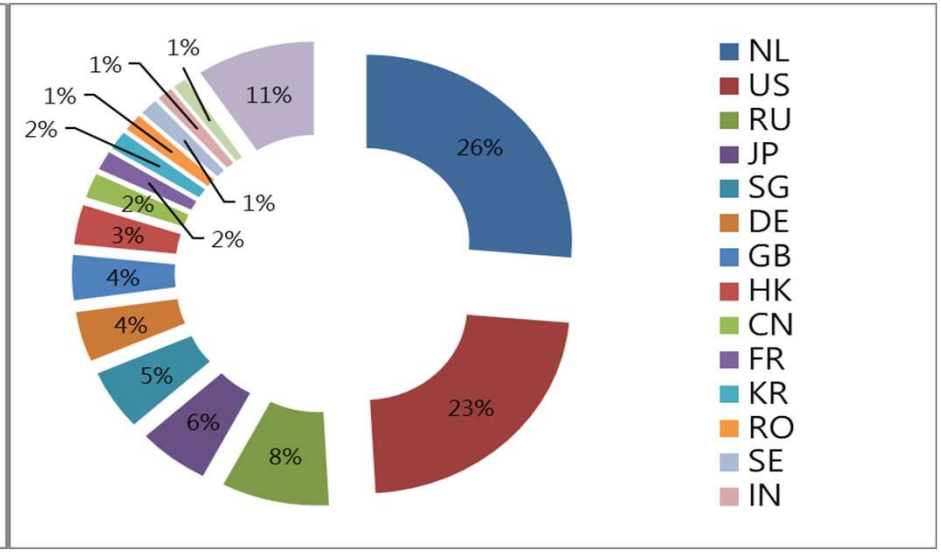
- 基於GO開發框架可快速編譯出不同設備之執行檔
- 使用漏洞高達25個，攻擊目標多為路由器或網路攝影機

聯防監控威脅情蒐(1/3)

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

- 112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93,895件、外交國防法務類之資訊蒐集74,721件及外交國防法務類之入侵攻擊68,757件
- 國外攻擊跳板來源前3名分別為荷蘭(26%)、美國(23%)及俄羅斯(8%)





聯防監控威脅情蒐(2/3)

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

- 網通設備為駭客攻擊目標
  - Citrix網通設備漏洞(CVE-2023-4966)資安風險分析

型號	版本
NetScaler ADC	12.1-FIPS至12.1-55.297
NetScaler ADC	13.1-FIPS至13.1-37.159
NetScaler ADC	12.1-NDcPP至12.1-55.297
NetScaler ADC與NetScaler Gateway	13.0 至13.0-91.13
NetScaler ADC與NetScaler Gateway	13.1 至13.1-49.13
NetScaler ADC與NetScaler Gateway	14.1 至14.1-8.50(不含)

受攻擊機關類別

資安責任等級 / 機關業務類別	A	B	合計
交通環境資源	2	0	2
經濟能源農業	1	1	2
教育科學文化	0	2	2
非行政院所屬	1	0	1
合計	4	3	7

  - 政府領域數位監視系統遭入侵成為殭屍網路案例分析

Mirai IoC	國別	自治系統名稱
194.124.213.44	NL	XTOM xTom GmbH, DE
45.32.25.125	JP	XTOM-AS-JP xTom, JP
45.117.103.223	JP	AS-CHOOPA, US

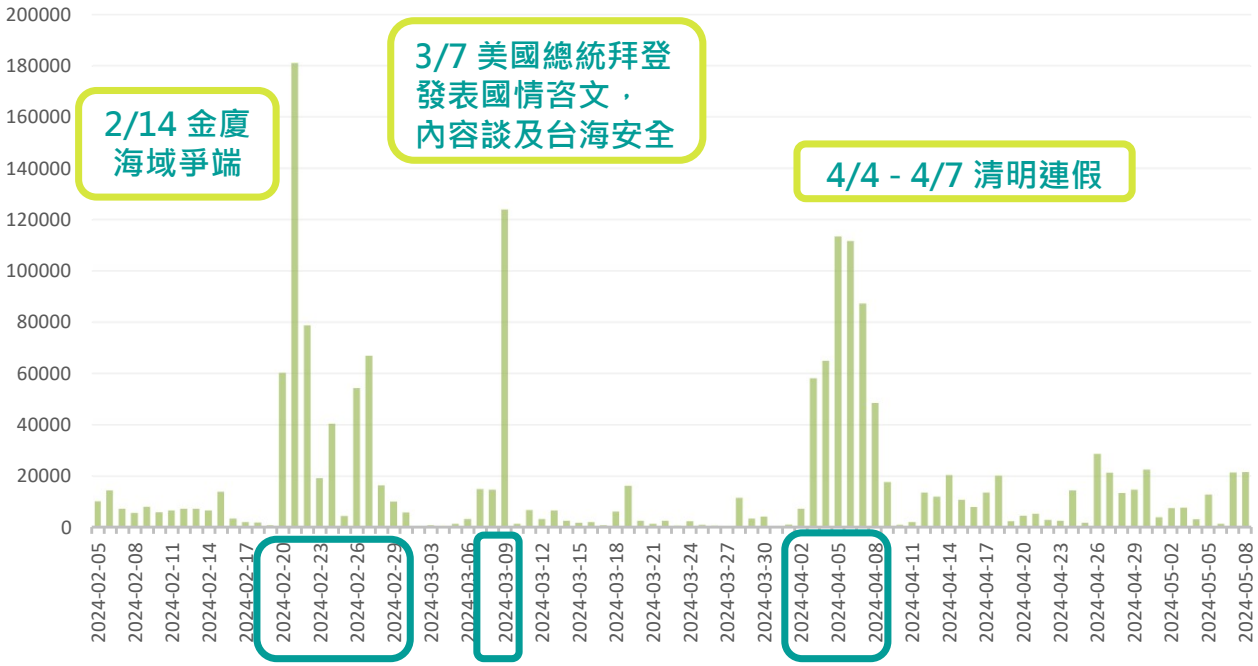
受攻擊機關類別

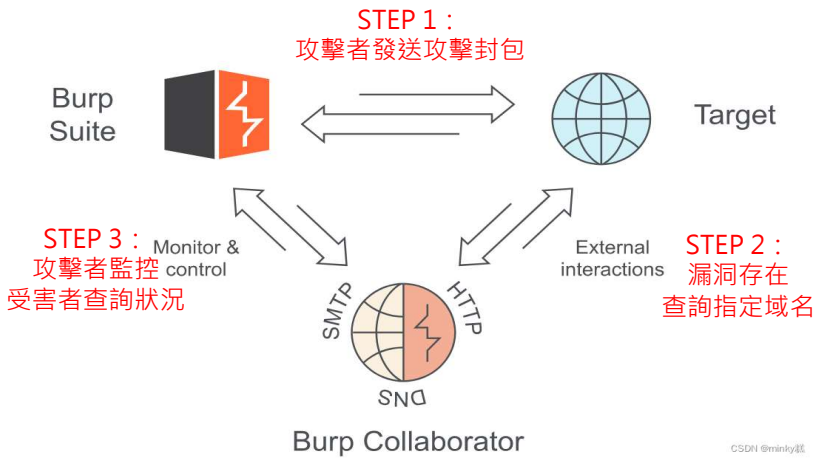
資安責任等級 / 機關業務類別	A	B	C	D	合計
綜合行政	2	8	48	33	91
內政衛福勞動	0	1	1	0	2
經濟能於農業	0	0	0	2	2
交通環境資源	0	2	0	0	2
非行政院所屬	0	1	0	0	1
合計	2	12	49	35	98

聯防監控威脅情蒐(3/3)

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

- Out-Of-Band 弱點掃描
  - 駭客利用Out-Of-Band方式對政府機關弱點掃描，可透過公開或自建之網域，供存在弱點設備報到，規避**防護設備阻擋掃描成功之回應**
  - 統計自113年2月5日起至113年5月8日止累計1,699,627筆攻擊連線，發現三波高峰，可能與特定時段或特定事件有關

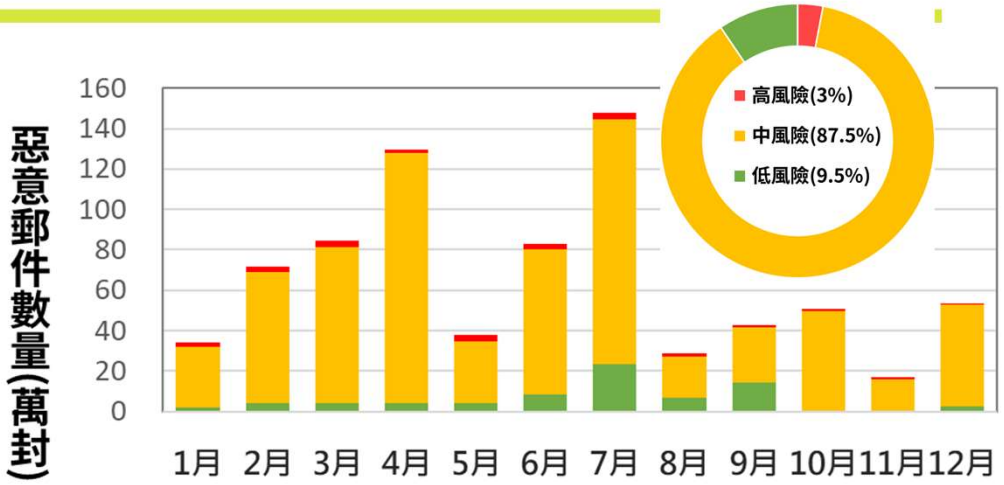




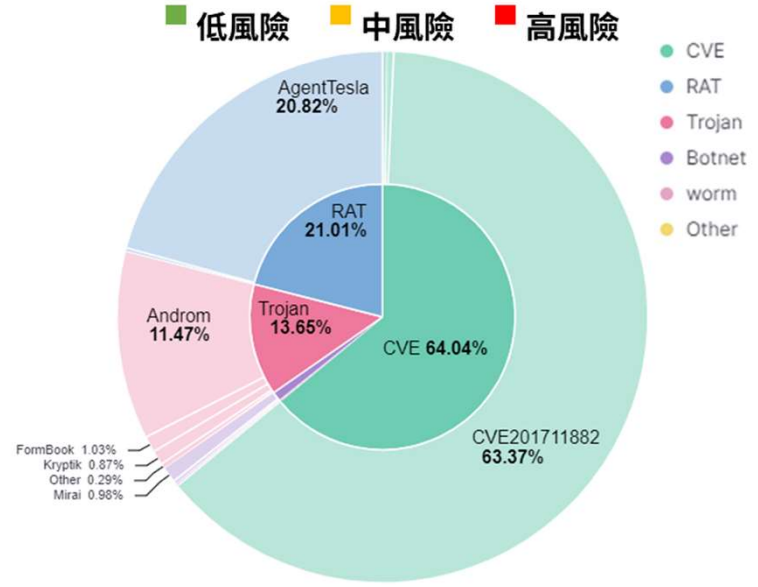
惡意電子郵件分析(1/2)

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

- 112年共檢測3.7億餘(378,784,437)封電子郵件，偵測發現**781萬餘(7,810,205)封可疑惡意電子郵件**，占2.06%



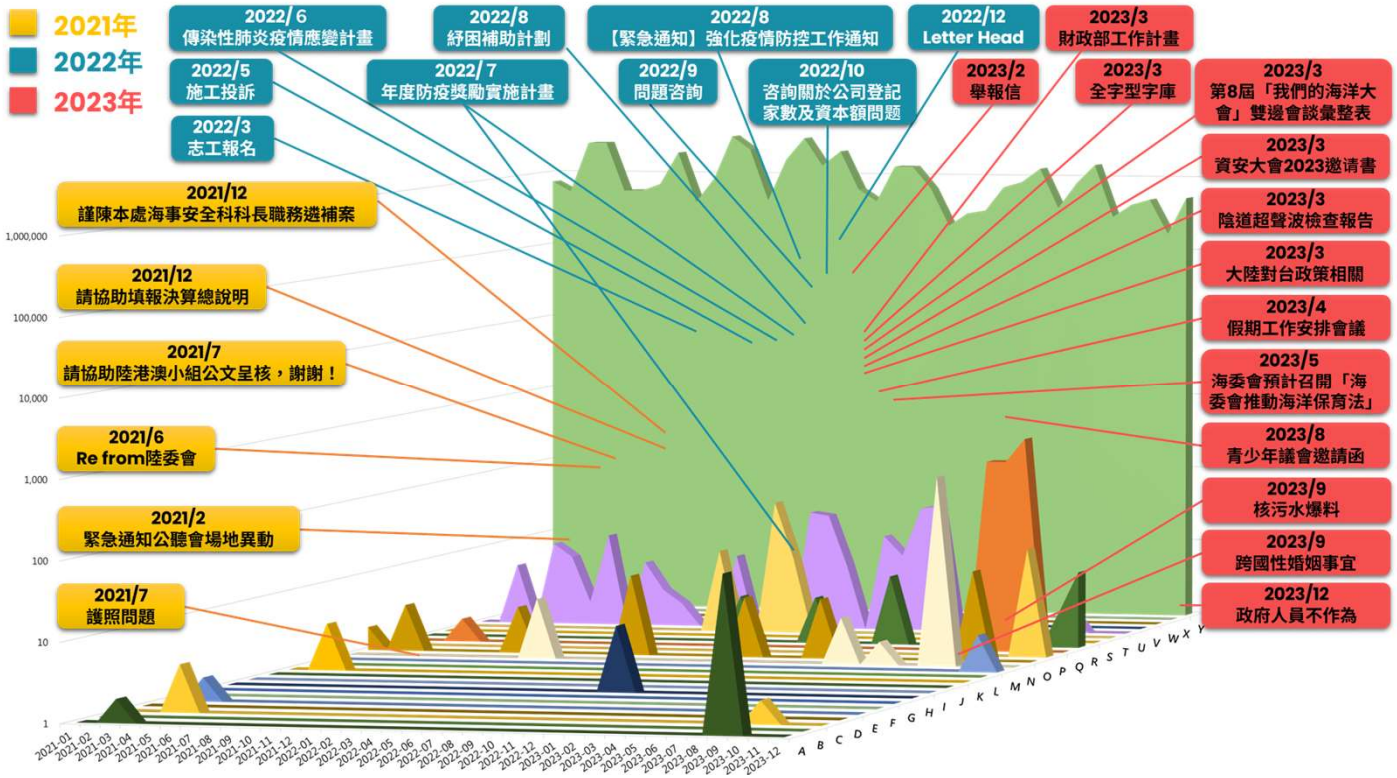
- 含惡意附檔之郵件中，以散布**CVE-2017-11882**漏洞利用之惡意文件最多，其次則為遠端木馬惡意程式，如**AgentTesla**與**Androm**等



惡意電子郵件分析(2/2)

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

- 112年政府領域APT郵件攻擊趨勢可歸納為**8波攻擊行動**，**計177封針對性社交工程郵件**，駭客利用檢舉爆料、會議邀請及業務諮詢等引誘性主旨，對政府機關人員發動攻擊



112年APT郵件攻擊手法

- 利用郵件系統之XSS零時差漏洞(CVE-2023-28705)
- 利用公務相關主旨搭配DLL Sideloading手法
- 濫用合法郵件服務與使用者互動之多層式攻擊策略
- 濫用短網址服務搭配公務諮詢之相關主旨
- 利用WinRAR之重大漏洞(CVE-2023-38831)
- 以投訴檢舉為由並利用離地攻擊手法下載Cobalt Strike後門程式

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

政府資安事件案例分析

近期常見資安事件

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

- 資訊資源向上集中擴大潛在影響範圍
- 物聯網/網通設備仍是常見攻擊標的
- 防護設備安全性與事件調查之挑戰
- 社交工程防不勝防隨時保持資安意識
- 落實上傳功能檢核機制防止惡意滲透

資訊資源向上集中擴大潛在影響範圍(1/2)

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

- 資訊資源向上集中政策確保資訊之統一管理，惟亦使資安事件發生時，影響範圍可能擴大至多個機關

案情提要

- 共構機房火災，導致網路與相關資通系統系統服務中斷
- 因網路與資通系統向上集中，連帶影響轄下多個單位對外網路與資通系統中斷，導致官網等對外服務中斷，內部亦無法收發電子郵件辦理業務
- 經切換備援網路後恢復網路服務，惟DNS服務未因服務向上集中增購，以致轄下單位雖恢復對外網路，但官網等對外資通系統仍無法正常解析恢復運作

資訊資源向上集中擴大潛在影響範圍(2/2)

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

- 推動資訊資源向上集中管理以強化資安，應同時考量「單點失效、全部失效」風險
- 模擬不同情境、部門與角色，定期辦理BCP演練，依據演練結果更新備援計劃，以期儘速恢復營運
- 備援用網路線路，頻寬或設定需與主線路一致

防護建議

- 依據風險等級、服務屬性或區域劃分，以避免可能之單點失效風險
- 機關皆有定期辦理BCP演練，建議避免單一類型或角色情境
- 備援用網路線路切換演練情境中，若涉及到DNS設定，建議納入設定SOP與設定啟用所需時間等

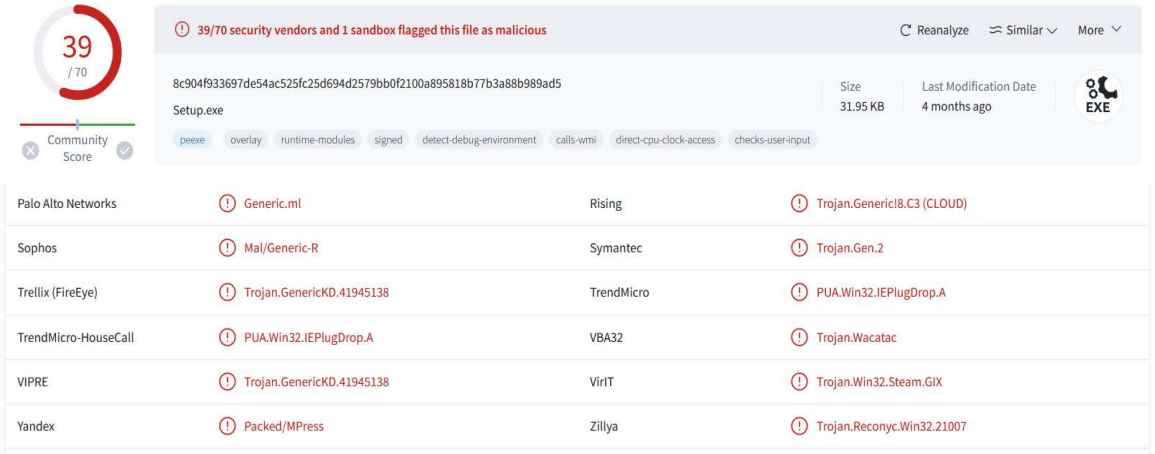
物聯網/網通設備仍是常見攻擊標的(1/3)

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

- 物聯網/網通設備通常具有較弱之安全性措施，並疏於更新與維護，仍然是常見之駭客攻擊目標

案情提要

- 資安院發現多個機關資訊設備存在惡意程式，發布警訊通知機關應處
- 機關通報表示受駭設備皆為監視器，機關多以汰換設備、下架或斷網處理



物聯網/網通設備仍是常見攻擊標的(2/3)

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

- 印表機或監視器等庶務設備，主要支援機關內部業務運作，開放外部網際網路存取，易受到未授權之存取或攻擊
- 設備可能存在預設密碼或漏洞，使得駭客可以輕易入侵並控制，進而進行各種攻擊

來源IP	來源Port	目的IP	目的Port	協定	應用	起始時間	結束時間	上傳	下載
外部IP	64071	機關IP	21	TCP	ftp	連線時間		1262	1081

案情提要

- 資安院發現多個機關資訊設備開啟FTP服務且遭上傳挖礦相關程式，發布警訊通知機關應處
- 部分機關機關通報表示受駭設備為印表機，並使用弱密碼或預設密碼，後續多以斷網處理

物聯網/網通設備仍是常見攻擊標的(3/3)

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

- 落實物聯網/網通設備密碼安全、定期更新，並實施防護措施與監控機制，以減少潛在風險與攻擊
- 評估設備開放網際網路存取之必要性，設置存取控制並關閉非必要之服務埠

防護建議

- 部分機關依資安考量，多以獨立專線設置監視器，惟缺少相關防護措施，建議設置防火牆或白名單限制存取來源
- 印表機等庶務設備，避免開放網際網路存取或使用弱密碼與預設密碼，關閉非必要之服務埠

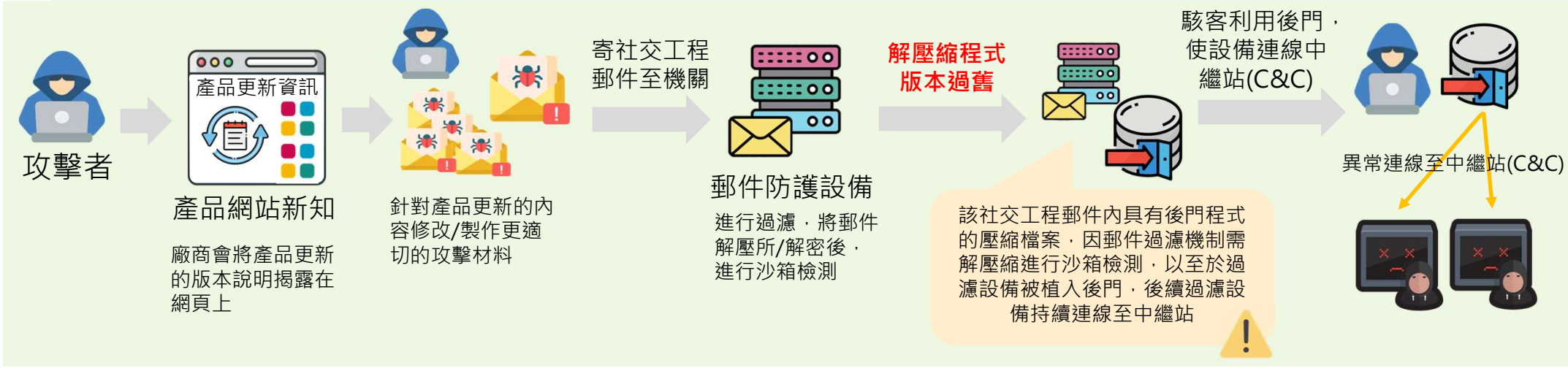
防護設備安全性與事件調查之挑戰(1/3)

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

- 郵件防護系統與防火牆等防護設備，同樣會成為駭客攻擊目標，探勘弱點並加以利用

案情提要

- 資安院偵測發現多個機關連線至中繼站(C&C)，發布警訊通知機關應處
- 機關通報表示連線設備皆為某廠牌之郵件防護系統，皆有定期進行安全性更新修補漏洞
- 經查該系統使用之第三方元件解壓縮程式，存在資安漏洞(CVE-2022-30333)遭利用，機關於更新修補漏洞前即遭駭客入侵植入惡意程式



防護設備安全性與事件調查之挑戰(2/3)

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

- 網通設備未能如電腦一樣，具備完整的系統事件與使用者資訊(如登入時間、檔案存取紀錄、程式執行紀錄等)，增加事件調查困難

案情提要

- 資安院偵測發現多個機關資訊設備產生可疑之連線，推判係防火牆遭攻擊
- 機關通報表示未能有明確日誌紀錄可供分析釐清事件原因

1. 惡意IP(45.77.33.174)疑似先攻擊防火牆port 541(預設開啟port)

起始時間	來源IP	來源Port	目的IP	目的Port	協定	Info
2024/4/10 17:47	45.77.33.174 攻擊IP	53648	機關IP	541	TCP	
2024/4/10 17:47	機關IP	19158	45.77.33.174 攻擊IP	80	TCP	POST /

2. 攻擊成功後受駭防火牆會POST回傳資料至攻擊IP(45.77.33.174) port 80/443
※惡意IP Port 80/443非正常網站，故無法瀏覽

防護設備安全性與事件調查之挑戰(3/3)

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

- 防護設備亦須即時更新，預防漏洞攻擊，並定期監控以早期發現異常
- 建議確認防護設備日誌記錄類型與內容，除掌握設備運行情形，亦可用以協助事件調查評估

防護建議

- 部分機關為確保更新不影響系統營運，於測試環境確認後再行更新正式環境，以致產生時間差，使得駭客有機會進行漏洞攻擊，建議因應漏洞訊息，可評估監控機制與防護措施
- 建議輔以設備運行日誌紀錄，做為事件調查參考，如連線當日是否有與平時不相同之紀錄產生

 # diagnose crashlog

```
2024-04-10 02:47:26 <00226> firmware FortiGate-80F v7.0.12 build0523b0523.230606 (
2024-04-10 02:47:26 <00226> application fgfmsd
2024-04-10 02:47:26 <00226> *** signal 11 (Segmentation fault) received ***
2024-04-10 02:47:26 <00226> Register dump:
2024-04-10 02:47:26 <00226> R0: 0000000004237758   R1: 0000000000000001   R2: 0000
2024-04-10 02:47:26 <00226> R3: 00000000ffffffff   R4: 0000007f81d1b000   R5: 0000
2024-04-10 02:47:26 <00226> R6: 0000000000000048   R7: fffffffffffffc0   XR: 0000
2024-04-10 02:47:26 <00226> R9: 0000007fdb937048   R10: 0000000008bc6c46   R11: 00
2024-04-10 02:47:26 <00226> R12: 0000000000000000   R13: 0000000000000020   R14: 0
                                                0050   IP0: 0000007f81c1cf10   IP1: 0
                                                000   R19: 0000000000000000   R20: 00
                                                0000   R22: 0000007fdb9355e0   R23: 0
                                                006e   R25: 0000000000001018   R26: 0
                                                006e   R28: 0000007fdb935218   FP: 00
                                                00000004237758   sp: 0000007fdb935090
                                                b2c   lr: 0000007f81c081c0
2024-04-10 02:47:26 pstate: 80000000 (NZCv daif -PAN -UAO)
```

 # diagnose debug crashlog read
xxxx: [Date & Time] .....
xxxx: [Date & Time] .....
xxxx: [Date & Time] .....

Format String Bug in fgfmd

CVE-2024-23113，FGFM具格式字串問題，可未經授權遠端執行指令

Summary

A use of externally-controlled format string vulnerability [CWE-134] in FortiOS fgfmd daemon may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests.

Version	Affected	Solution
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above

IR Number	FG-IR-24-029
Date	Feb 8, 2024
Severity	Critical
CVSSv3 Score	9.8
Impact	Execute unauthorized code or commands
CVE ID	CVE-2024-23113

社交工程防不勝防隨時保持資安意識(1/2)

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

- 社交工程攻擊為常見攻擊手法之一，通過欺騙或誘導人員，以取得機敏資訊或存取權限等其他惡意行為，如誘騙郵件或偽造網站

案情提要

- 資安院偵測某政府機關有偽冒程式之異常連線
- 調查發現是機關同仁於公務電腦安裝Telegram程式，透過Google搜尋發現有中文版，惟下載了偽冒的安裝檔，導致公務電腦受駭

防護建議

- 公務設備不應安裝非公務使用軟體
- 如因業務需求安裝軟體，應於官方網站下載為佳
- Telegram官方迄今尚未提供中文版
  - ✓ 偽造之Telegram軟體係由Google協作平台架設之網站：網址開頭為site.google.com

社交工程防不勝防隨時保持資安意識(2/2)

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

- 社交工程攻擊成功主因，除人員缺乏足夠資安意識識別與防範之外，人員存在僥倖心態亦容易遭攻擊成功

案情提要

- 資安院偵測發現某機關出現惡意程式行為特徵之異常連線，調查發現機關資訊助理為執行檢測，誤下載了被加料的檢測軟體，導致公務電腦受駭

防護建議

- 官方網站 所提供的檔案較有保障
- 因為僥倖心態刻意瀏覽部落格資訊，卻下載了加料檔案，得不償失

落實上傳功能檢核機制防止惡意滲透

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

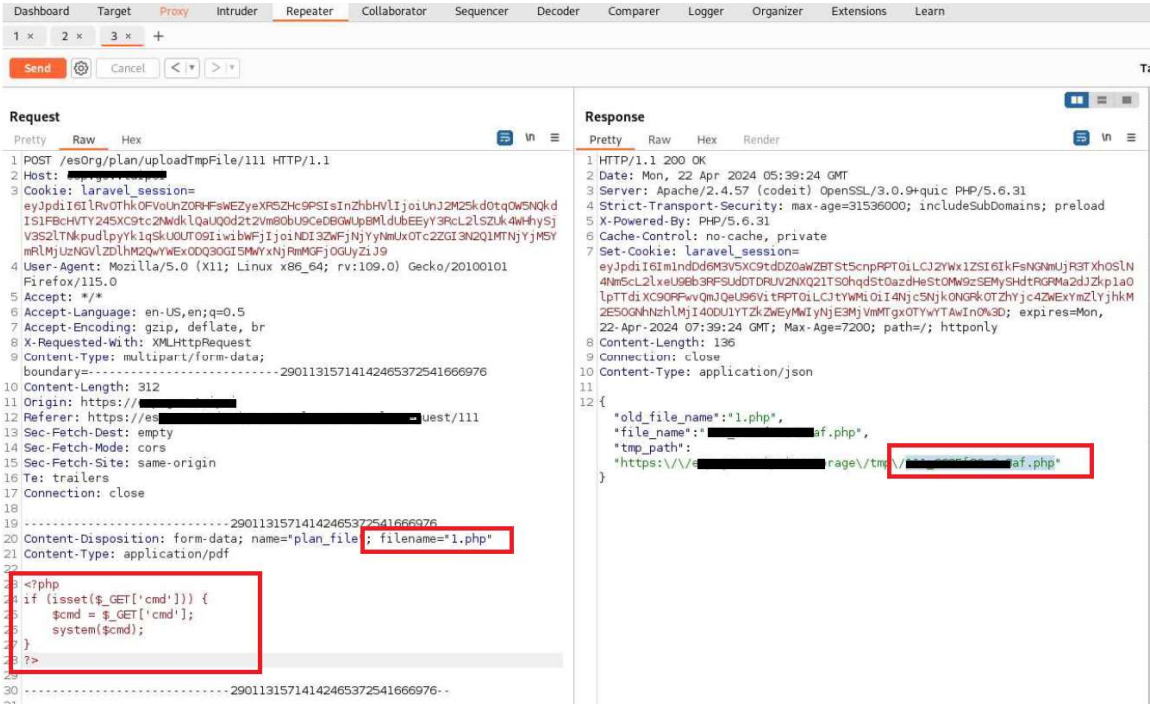
- 網站前端檔案檢查雖然能夠在使用者上傳檔案時，快速檢測與過濾不合規之檔案，惟存在被繞過之風險

防護建議

- 落實Client端嚴格檢查上傳之檔案，限制使用者上傳格式，確實檢查檔案格式
- Server端檢查機制，補充前端檢查的不足，如檔案目錄設定為不可執行，提高不安全檔案的防範能力
- 遮蔽上傳路徑，防止駭客獲取檔案真實位置，避免駭客存取

案情提要

機關網站上傳功能，可利用工具攔截封包，修改「filename」參數內容，將pdf改為php，並插入語法



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

強化內部管理妥善因應內外環境變化

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

- 持續提升人員資安意識
  - 依角色別加強人員資安訓練
  - 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，如密碼暴力破解登入或其他異常活動跡象
  - 持續關注生成式AI發展，及早預防針對性社交工程攻擊
- 規劃並落實雲端服務資安防護措施
  - 採用雲端服務時，應成立專案指派人員進行規劃與管理，納入ISMS 及日常資安管理作業中
  - 參考「政府機關雲端服務應用資安參考指引」

加強設備盤點防堵資安破口

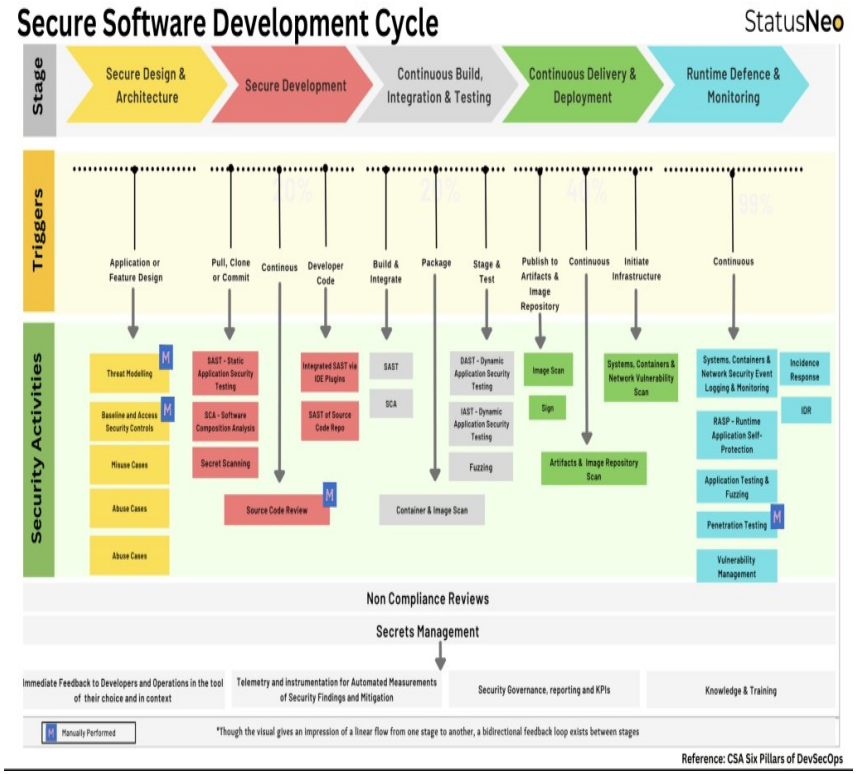
國家資通安全研究院
National Institute of Cyber Security

- 落實資產管理與弱點修補
  - 未能妥善納入盤點之資訊設備，如門禁系統與網路攝影機等物聯網設備，常成為駭客入侵起點
  - 無更新支援之設備應強化資安控制措施，並盡速規劃汰換
  - 配合資通安全弱點通報機制(Vulnerability Alert and Notification System, VANS)，及時進行漏洞修補與安全性更新
- 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，並符合密碼複雜度要求

資通系統資安從規劃開始

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

- 資通系統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
  - 落實上傳功能檢核機制
  - 採用多因子身分鑑別機制
  - UI(Web或Win Forms)及API，開發時應同時考量對應之風險
- 資通系統建置應落實上線前資安檢測
  - 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
  - 資通系統權限開放情形，應納入上線前之檢驗項目
- 資通系統與服務委外須落實供應商管理



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

強化政府數位韌性

政府數位韌性巡航健檢

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

- **健檢之目標**
  - 在變動或極端的環境下，**系統持續提供服務**並能在故障時復原
  - 系統**易用性** × **可維護性** × **高可用性**
- **系統健檢效益**
  - **提升政府數位服務品質**
    - **資通訊應用計畫**所規劃**新建或調修的系統**：協助政府於系統規劃階段，將網路高可用、系統架構擴充性、系統承載量、上線前壓力測試、應變計畫等事項納入考量，強化系統韌性
    - **政府現有系統**：找出系統服務的痛(盲)點，並提出解決方案，增強資訊系統持續運作能力
  - **擴大政府數位基礎建設**
    - 尋求**政府資訊系統升級為數位基礎建設**之機會
      - 113年度公共建設計畫，新增「數位基礎建設」類別
      - 獲選為全國示範數位韌性系統，且成為數位基礎建設，**具爭取公共建設計畫預算之機會**

112年巡航健檢精進意見-共通性建議(1/2)

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

- **易用性**
  - 部分網站隱私權保護政策與網站行為不一致，建議機關放置 YouTube 影片時，將廣告功能移除
  - 處理措施
    - 教材：https://github.com/nics-tw/resilience-material/blob/main/usability.md
    - 放置YouTube 影片，需申請**非營利組織並關閉廣告功能**，以保護使用者資料
- **可維護性**
  - 廠商交付的原始碼與弱點掃描報告，機關需有獨立的驗證與佈署流程
  - 建議機關建立自動化驗證與佈署流程，並使用工具來管理與掃描系統元件組成與可能弱點
  - 處理措施
    - 教材： https://github.com/nics-tw/resilience-material/blob/main/maintainable.md
    - **建立原始碼管理平臺**，並請廠商將程式碼交付於機關原始碼管理平台內，以利開始進行自動化驗證與佈署流程規劃

112年巡航健檢精進意見-共通性建議(2/2)

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

- **高可用性**
  - 機關機房除搭配各電信廠商外，仍需要瞭解電力、冷卻方式等機房管理方式，若發生異常事件時，方能即時反應
  - 網路邏輯設定須更明確，例如網域安全設定(DNS)是否合適、是否需要分散式網站內容(CDN)服務、本地網路韌性是否足夠等
  - 處理措施
    - 教材： https://github.com/nics-tw/resilience-material/blob/main/high-availability.md
    - 依據政府機關(構)資訊機房環境安全自檢表進行**機房管理**項目的檢視
    - 針對**公有雲廠商檢視**服務層級協議（Service Level Agreement，SLA）建議每月達到 99.99%
    - 依照**災害恢復狀況**進行網路邏輯設定**檢視與調整**，如：DNS 的存留時間（Time to live，TTL）設置為較短的時間(如300 秒)，以縮短 DR 站點上線切換的時間

如有問題，歡迎來電國家資通安全研究院(02)6631-1822 或來信至maowang@nics.nat.gov.tw 詢問!

資料來源：國家資通安全研究院網站「核心業務\數位韌性教材」https://www.nics.nat.gov.tw/core_business/digital_resilience/Digital_Resilience_Materials

結論與建議

結論與建議

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

- 政府機關一直是駭客組織鎖定之攻擊目標，各機關須持續加強人員資安意識，防範APT惡意電郵攻擊
- 連網設備仍常見預設帳密問題，應持續宣導改善
- 設備管理介面常具備網路工具，有高機率存在命令注入漏洞，須加強管理
- 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
- 因應全球資安風險，持續加強下列各項工作
  - **擴大資安聯防**：進行資安聯防，並落實資安責任等級應辦事項，以強化防禦能力
  - **加強資安韌性**：建構關鍵資訊基礎設施防護(CIIP)框架，加強資安韌性
  - **檢測工業控制系統**：研發工業控制系統資安檢測技術，精進各CI領域工控系統管理

報告完畢 敬請指教

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