政府機關資安威脅與防護重點

行政院國家資通安全會報技術服務中心

111年11月

【普通】

大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

全球資通安全威脅趨勢

- 綜整111年全球資安威脅報告[1-11]，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

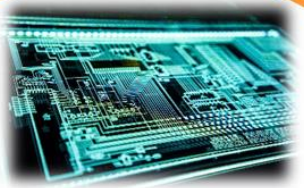
社交工程手法
層出不窮

進階持續性攻擊
竊取機敏資料

漏洞利用攻擊
風險激增

雲端服務平台
遭駭客濫用

資安(訊)供應商
遭駭破壞供應鏈
安全



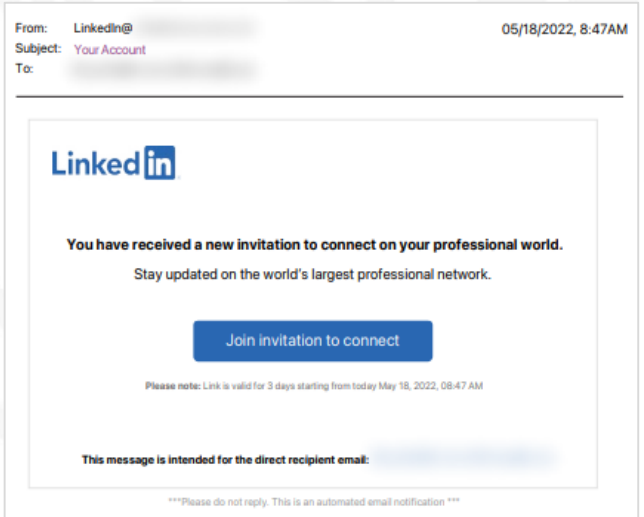
萬物聯網
資安風險倍增

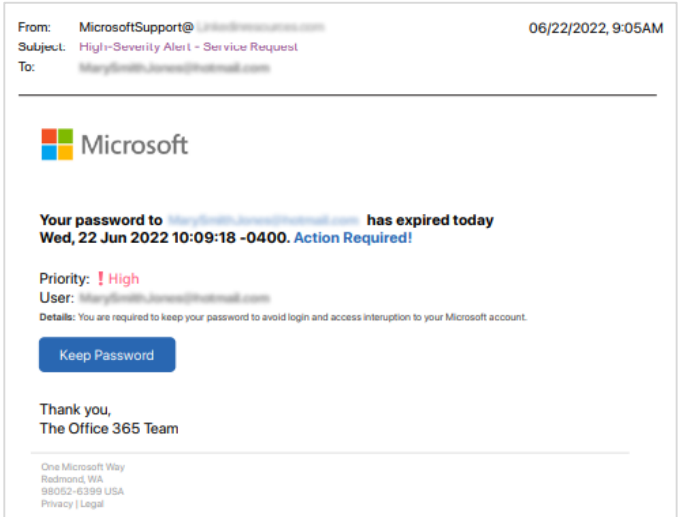
發令與控制

採取行動

社交工程手法層出不窮

- 據統計，社交工程電子郵件攻擊占比第一為釣魚攻擊(Phishing)，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)
  - 資安廠商Abnormal Security[1]111年H2報告指出，共計超過265個大眾熟悉品牌常遭利用於釣魚攻擊，其中以社群網路登入與微軟相關產品最常被偽冒，以騙取個人機敏資訊
  - 資安廠商Trellix[12]指出111年美國選舉之惡意電子郵件大幅增加，駭客藉選舉之際，透過釣魚攻擊騙取選舉工作人員帳號密碼





進階持續性攻擊竊取機敏資料

- 進階持續性攻擊(APT)為駭客集團鎖定特定組織或國家，精心策劃結合多種攻擊手法，包括：社群平台、手機、Office文件及各式產品漏洞，持續而隱匿地逐步滲透，藉此竊取機敏資料
  - 111年9月，微軟揭露北韓駭客組織Zinc[2]利用LinkedIn平台建立招募員工假檔案，鎖定英、美及印度國籍之工程師，要求求職者以WhatsApp通訊，透過手機通訊管道遞送已被植入後門之惡意檔案
  - 111年9月， 資安廠商DuskRise指出俄羅斯駭客組織APT28[3]利用PowerPoint簡報檔案散布惡意軟體Graphite，針對歐盟、東歐國家政府部門與國防單位進行攻擊
  - 111年9月，資安廠商Recorded Future指出中國駭客組織[4]利用Sophos防火牆產品漏洞(CVE-2022-1040)與微軟Office文件漏洞(CVE-2022-30190)，針對西藏社區組織與個人發動攻擊

遠端程式碼執行漏洞仍頻繁

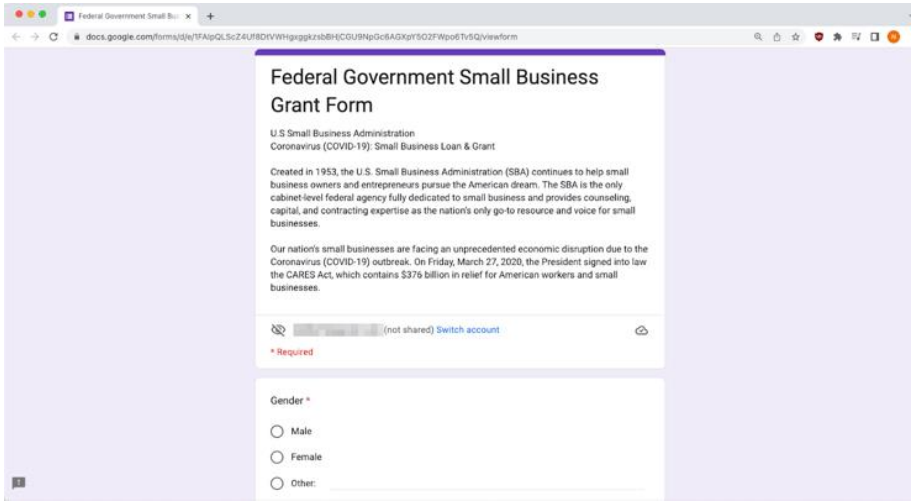
- 參考近年美國網路安全及基礎設施安全局(CISA)漏洞報告[5][6]與資安廠商INFOSEC發布之111年最危險漏洞資訊[13]
  - 駭客最愛利用漏洞主要為遠端程式碼執行或提權等權限控管缺陷
  - 另商用軟體Exchange伺服器產品等重大漏洞也屢被利用

CISA公布之10大常用漏洞				
漏洞代號	CVE編號	CVSS分數	漏洞類型	APT攻擊常用
Log4Shell	CVE-2021-44228	10(Critical)	RCE	V
N/A	CVE-2021-40539	9.8(Critical)	RCE	V
ProxyShell	CVE-2021-34523	9.8(Critical)	Elevation of privilege	
	CVE-2021-34473	9.8(Critical)	RCE	
	CVE-2021-31207	7.2(HIGH)	Security feature bypass	
ProxyLogon	CVE-2021-27065	7.8(HIGH)	RCE	V
	CVE-2021-26858	7.8(HIGH)	RCE	V
	CVE-2021-26857	7.8(HIGH)	RCE	
	CVE-2021-26855	7.8(HIGH)	RCE	
N/A	CVE-2021-26084	9.8(Critical)	Arbitrary code execution	

Microsoft Exchange Server相關漏洞

雲端服務平台遭駭客濫用

- 雲端服務平台可幫助企業組織快速部署提高效率，但也遭駭客利用以掩飾惡意行為
  - 趨勢科技「2022 Midyear Cybersecurity Report」報告[7]指出，現今駭客常使用雲服務進行隱匿通訊(Cloud Tunneling)，除減少建置永久性網路基礎架構之需求，也不需特意掩蔽真實來源IP位址
    - Cloudflare, Google Cloud Platform, AWS, 微軟Azure, 阿里雲, 騰訊雲等
  - 駭客利用合法雲服務網域(Domain)建置釣魚頁面，以規避偵測
    - 因應疫情，駭客濫用Google表單並搭配釣魚電子郵件，蒐集受駭者個人資料[14]
    - 駭客濫用AWS建置與託管釣魚網站頁面，以騙取個人帳密[15]



駭客濫用Google表單蒐集個資

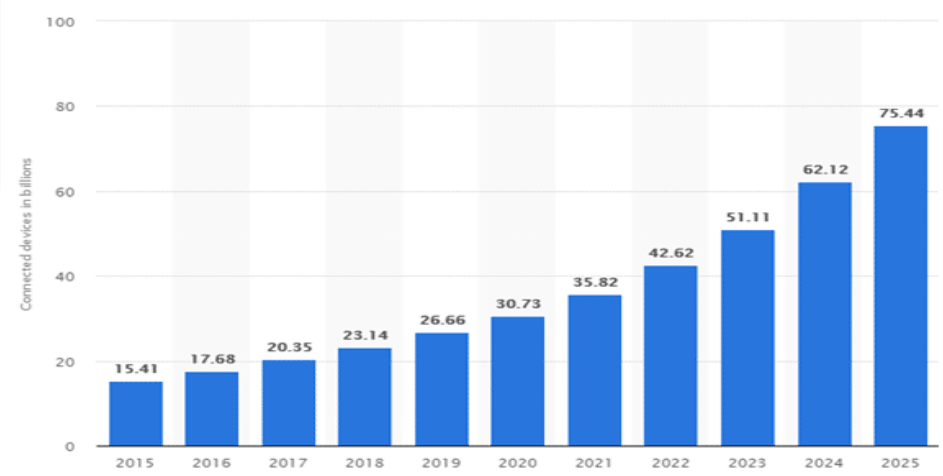
駭客持續破壞供應鏈安全

- 供應鏈風險對全球組織影響漸增，供應鏈安全落差使駭客鎖定監控較不嚴謹之設備或供應商，做為入侵管道
  - ISACA「全球供應鏈安全差距」調查報告[8]顯示，全球25%組織在過去1年內皆曾遭受供應鏈攻擊
  - 111年1月，身分驗證及存取管理業者Okta之第三方廠商Sitel工程師筆電遭駭[9] [16]，導致Okta客戶資料外洩，包含Nvidia與三星等，並使微軟遭駭客入侵
  - 111年2月，台灣金融業曾遭軟體供應鏈攻擊[10]，利用金融業常用證券軟體管理介面漏洞入侵，並安裝後門程式意圖竊取資料

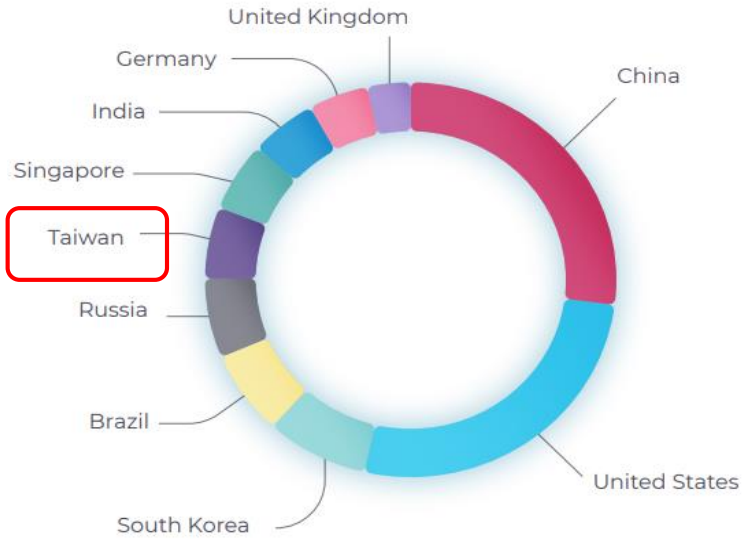
最擔憂會影響組織之供應鏈風險		
1	勒索軟體	73%
2	供應商資安落實程度不佳	66%
3	軟體漏洞	65%
4	第三方儲存	61%
5	第三方供應商可存取到資訊系統	55%

萬物聯網受駭風險倍增

- 因物聯網設備普及，多數物聯網裝置缺乏有效控管，長期遭駭客入侵利用於各種攻擊，如DDoS攻擊與殭屍網路
  - IOT Business News [18]指出111年物聯網主要威脅包括：
    - ➢ 殭屍網路與惡意物聯網設備
    - ➢ 弱密碼與身分驗證機制不足
  - Nozomi Networks Labs[11]在111年上半年OT/IOT安全報告中指出，駭客最常透過SSH與Telnet協定存取安全性不足之物聯網設備



IOT設備成長趨勢[17]



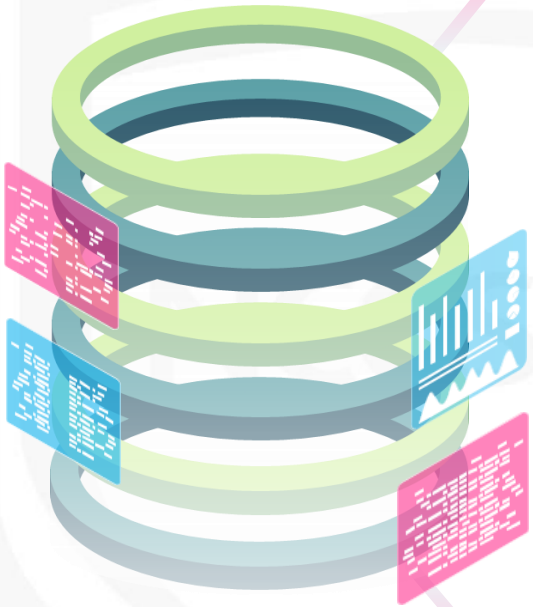
駭客利用受感染IoT設備發起網路攻擊之主要國家

大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

政府領域資安威脅趨勢

- 綜整111年政府領域資安威脅偵測與機關通報資訊，主要威脅趨勢有6大面向



1.社交工程與APT惡意電子郵件仍為主要攻擊手法

2.遠端服務探測與產品漏洞利用為主要網路威脅

3.雲端服務中繼站盛行協助駭客隱匿惡意行為

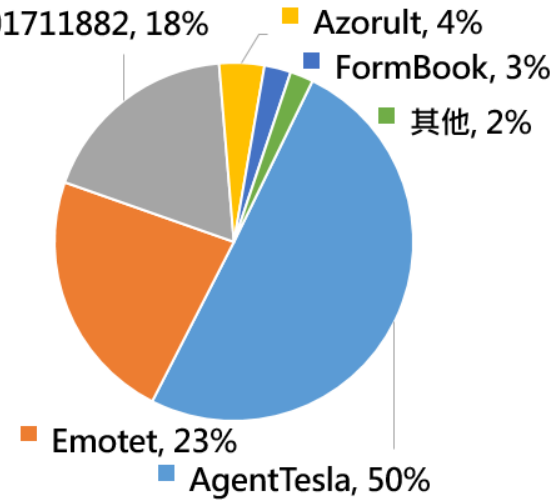
4.萬物聯網衍生應用造成資安風險

5.供應鏈安全遭破壞成為入侵跳板

6.人員資安意識不足導致資料外洩

偽冒政府機關發動社交工程攻擊

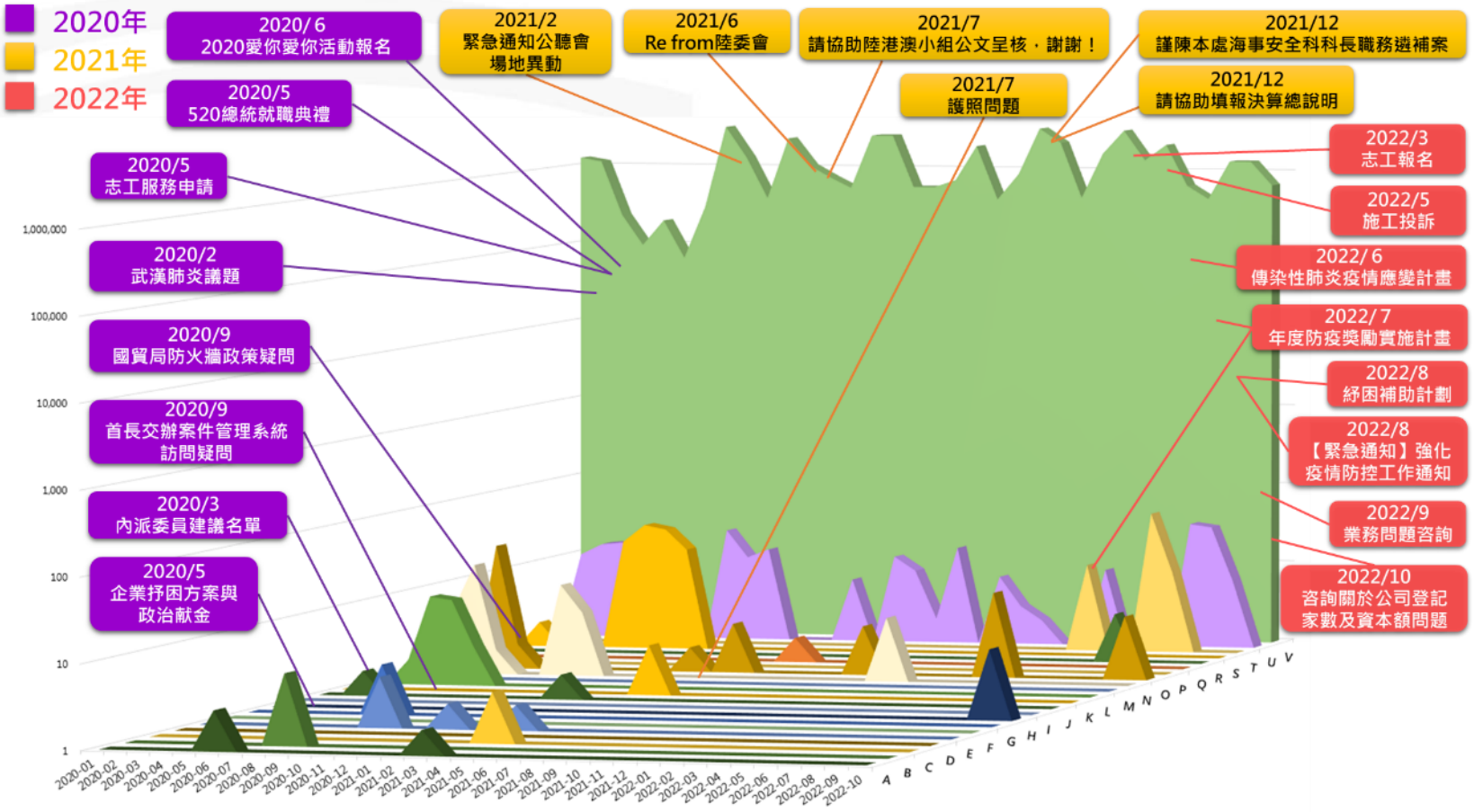
- 111年7月至９月，駭客大規模散布假衛福部紓困訊息，騙取民眾身分個資與網路銀行資訊
  - 偽冒衛福部與政府機關之域名(xxxgov.tw)，架設假官方釣魚網站
- 上半年Emotet仿真郵件大幅增加外，全年度含惡意附檔之惡意電子郵件以散布遠端木馬(AgentTesla)最多
  - AgentTesla於2014年發現，專門竊取機敏資訊，110年2月發現新的變種後，相關攻擊持續顯著增加



TOP5郵件附檔惡意程式

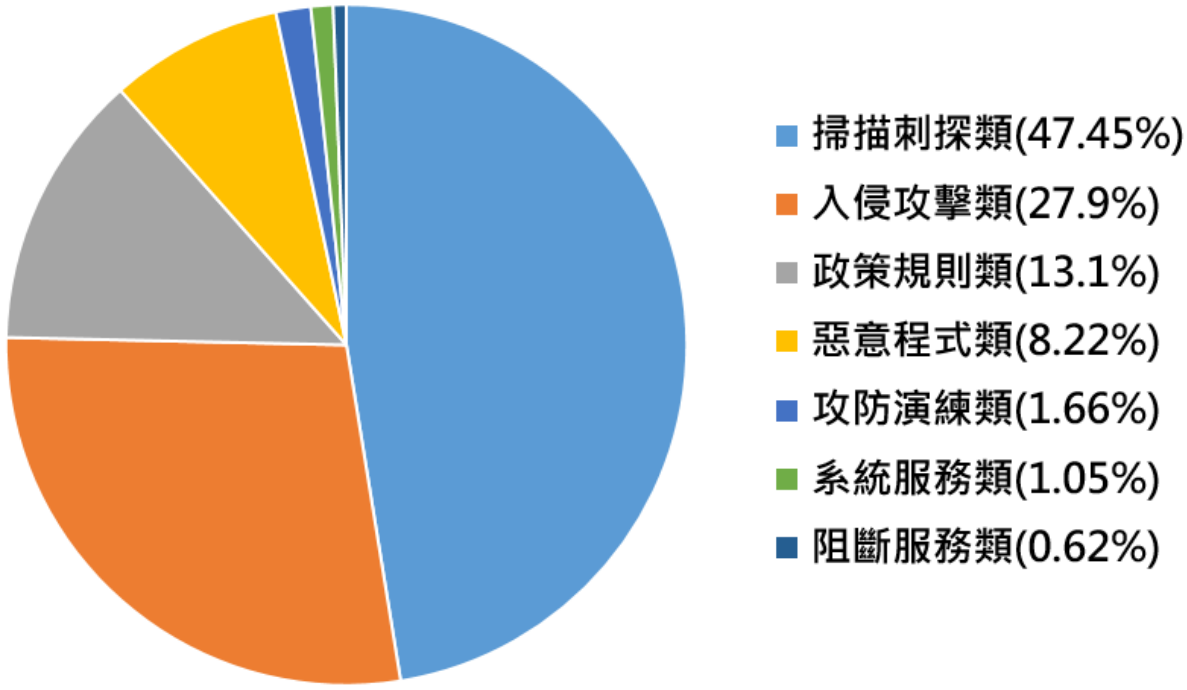
進階持續性攻擊鎖定業務窗口

- 111年政府領域APT惡意電子郵件攻擊，駭客持續寄送含惡意附檔之電子郵件，以新冠疫情、業務諮詢等郵件主旨，對政府機關發動魚叉式社交工程郵件攻擊



遠端服務探測與產品漏洞威脅

- 111年1月至9月政府骨幹網路主要威脅類型
  - 掃描刺探類(47.45%)，大多為針對已知漏洞、遠端服務(如RDP遠端桌面連線)及密碼猜測之探測行為
  - 入侵攻擊類(27.9%)，主要針對網頁應用程式之攻擊行為



政府骨幹網路攻擊分布趨勢統計

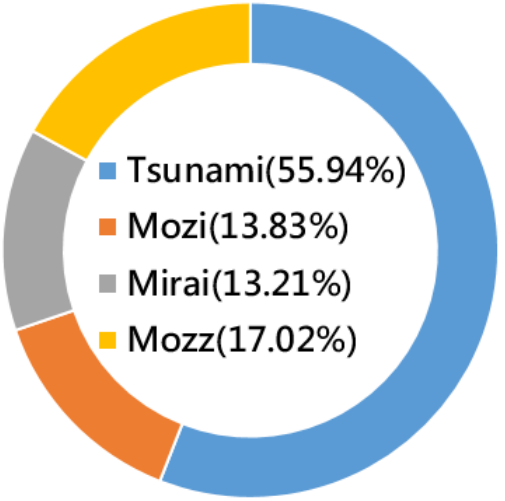
濫用雲端服務建置中繼站盛行

- 近兩年駭客時常使用紅隊演練工具，產製Cobalt Strike後門程式，並搭配雲端服務建置中繼站以使用合法IP位址與域名進行資料竊取，藉此規避資安防護偵測機制
  - 駭客透過域名隱匿(DNS Tunneling)與HTTP Beacon通訊兩種方式，將惡意傳輸流量隱藏於合法流量中
  - 常遭利用雲端服務，包括：Cloudflare、AWS、Azure及騰訊雲等

- **Cloudflare(4)**
  Cobalt Strike(3)
  –綜合行政
  Too hash(1)
  –外交國防法務
- **Cloudflare(3)**
  Cobalt Strike(3)
  –綜合行政
  –交通環境資源
- **Cloudflare(5)**
  Cobalt Strike(5)
  –非行政(府、四院及其所屬)
  –綜合行政
  –外交國防法務
- **Cloudflare(2)**
- **AWS(2)**
- **Azure(1)**
- **騰訊雲(1)**
  Cobalt Strike(5)
  –內政衛福勞動
  Plead(1)
  –經濟能源農業

萬物聯網衍生資安風險

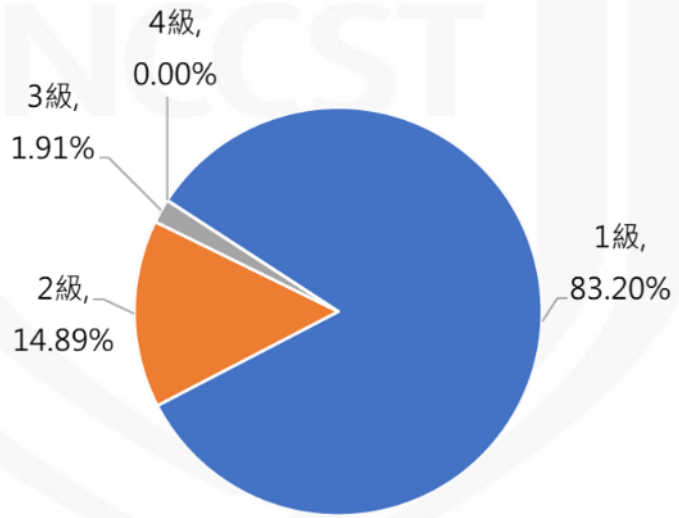
- 111年上半年透過蜜網誘捕網路攻擊，針對物聯網設備之網路攻擊共計餘3千萬次(30,517,068)，以Mirai殭屍網路為主，包括變種Tsunami共占69.15%，顯見暴露於網際網路之物聯網設備仍存在大量資安風險
  - 攻擊來源受駭裝置經分析後大多為路由器與網路錄影設備，少量網頁應用服務、網路儲存裝置等類型

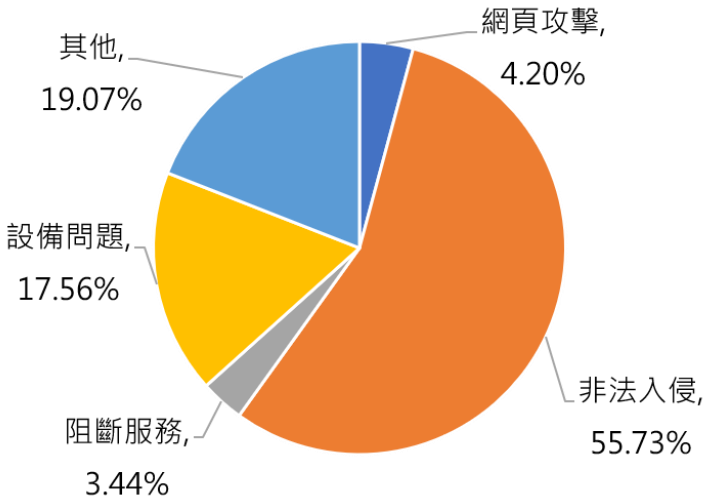


- 111年8月美國聯邦眾議院議長裴洛西訪台，駭客對台發動網路攻擊，入侵車站與高鐵等關鍵基礎設施之連網電子看板
  - 缺乏適當資產存取管控與弱點補強

供應鏈安全遭破壞成入侵跳板

- 111年1月至10月共接獲524件之通報事件，仍以1級資安事件為主，惟於非法入侵事件中發現，因供應鏈安全落差成為駭客入侵跳板，導致機關遭入侵
  - 以非法入侵為大宗占55.73%，部分事件肇因於供應鏈廠商維護環境或管理疏失、社交工程及使用者行為，其次為設備問題，例如興達發電廠3月停機事件影響多個政府機關可用性問題
  - 42.56%(223件)為機關接獲技服中心警訊通告後所進行之通報

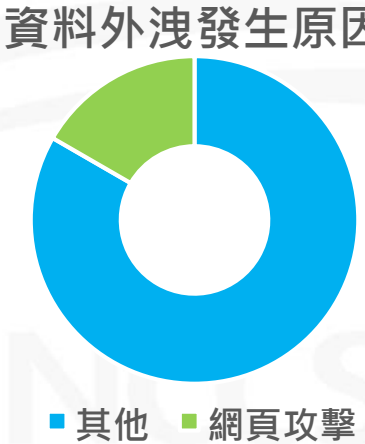




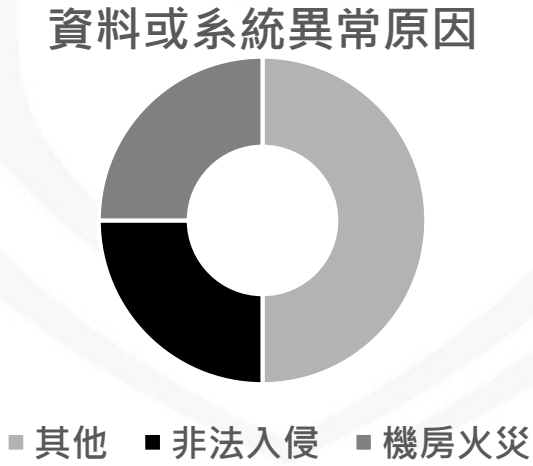
※統計區間：111/1/1至111/10/31公務機關通報(不含實兵演練)統計

人員資安意識不足造成威脅

- 111年1月至10月共10件之3級資安通報事件，造成之影響為資料外洩與資料或系統異常，分析其發生原因發現造成資料外洩之主因為人員資安意識不足



- **人員疏失**，誤將未遮蔽之個資公開或錯置
- **點擊釣魚訊息**，導致管理者帳號密碼遭竊，進而取得對話內容中之個資
- **前員工濫用權限**，撈取機關人員個人資料並進行兜售



- **密碼遭暴力破解**，攻擊者入侵後刪除477筆資料
- **軟硬體異常**，導致資料異常刪改或系統緩慢
- **機房火災**，設備吸入滅火粉塵致故障

大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

新冠疫情社交工程攻擊案例

- 駭客利用國人關注新冠肺炎議題，以提供紓困福利為由，架設偽冒衛福部與相關政府域名釣魚網站，散布釣魚郵件與手機惡意應用程式，對政府機關與一般民眾無差別發動攻擊，進行個人資料與網路銀行詐騙

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認政府相關域名之正確性，勿隨意提供機敏資訊

偽冒機關帳號散布惡意電郵案例

- 駭客利用政府機關電子郵件伺服器未設定寄件者原則架構(SPF)，大規模偽冒政府機關人員電子郵件帳號，發送大量惡意勒索電子郵件進行社交工程攻擊
  - 111年9月偵測發現，遭駭客偽冒之政府機關，共計87個政府機關、117機關域名未完善SPF設定

未設定SPF之機關責任等級分布	
A級機關	6
B級機關	27
C級機關	38
D級機關	13
其他	3(資安法尚未列管)

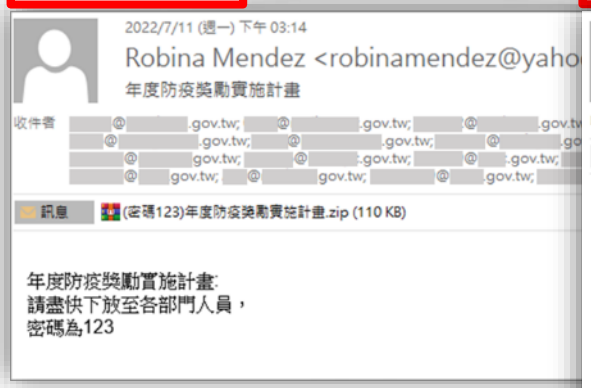
防護建議

- 建議可參考寄件者原則架構(SPF)設定，完善郵件安全防護，避免機關電子郵件帳號遭偽冒利用

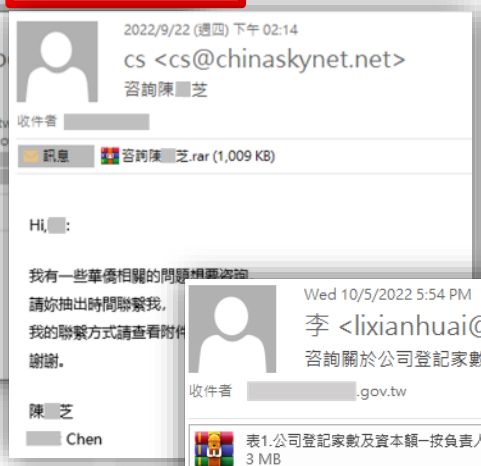
進階持續性攻擊郵件案例(1/2)

- 除新冠肺炎議題相關攻擊外，組織型駭客針對政府機關業務負責窗口，以業務諮詢相關問題為主旨，搭配惡意附檔，發動魚叉式社交工程攻擊

新冠議題



業務諮詢



防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 確認電子郵件附檔屬性或檔名後才點擊檔案，提高警覺

進階持續性攻擊郵件案例(2/2)

- 組織型駭客偽冒技服中心，於郵件中安插技服中心圖示並使用「資安審查」等郵件主旨，針對台灣企業發起魚叉式社交工程釣魚郵件攻擊

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件與連結
- 如感覺有異請先洽技服中心查證，可以利用通報網站或技服信箱進行情資分享

產品漏洞威脅案例

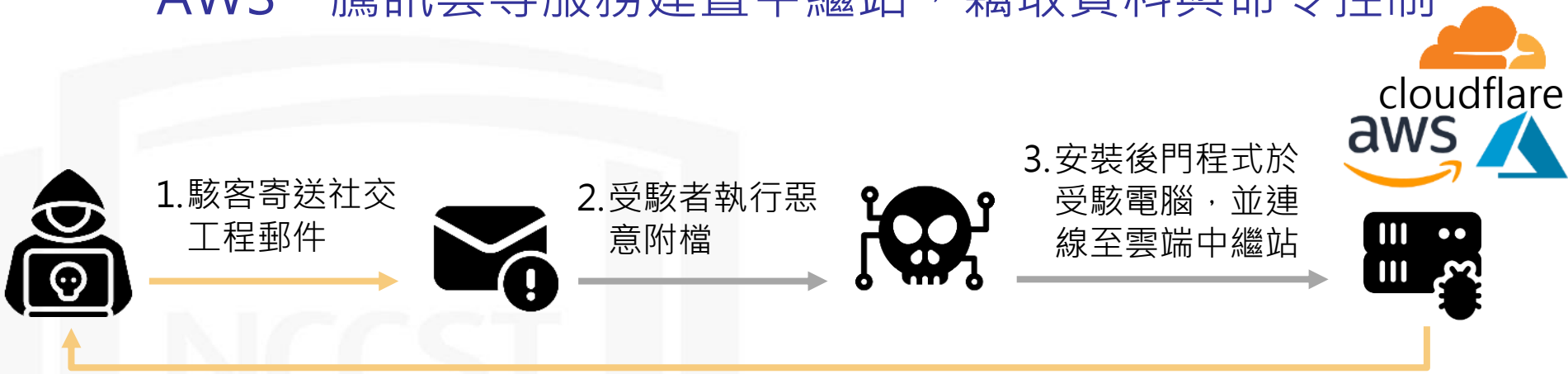
- 網通設備產品一向為駭客鎖定之攻擊目標，111年初F5之BIG-IP產品發現重大安全漏洞(CVE-2022-1388)，可透過iControl REST身分鑑別漏洞存取BIG-IP系統，並遠端執行任意程式碼
- 經異常連線行為偵測，發現某機關疑似受駭，經鑑識調查後，發現駭客利用BIG-IP漏洞入侵該設備以放置後門程式與駭客工具，意圖遠端操控並進行內部橫向擴散

防護建議

- 儘速下載對應版本之更新檔，並將管理頁面功能更新至最新版本
- 若版本因已停止支援而未釋出修補程式，建議升級至仍有支援且已推出修補程式之版本
- 若無法更新至最新版本，請採出官方所建議之緩解措施

雲端服務中繼站威脅案例

- 110年偵測多起進階持續性郵件攻擊，駭客使用紅隊演練工具產製Cobalt Strike後門程式，搭配Cloudflare、AWS、騰訊雲等服務建置中繼站，竊取資料與命令控制

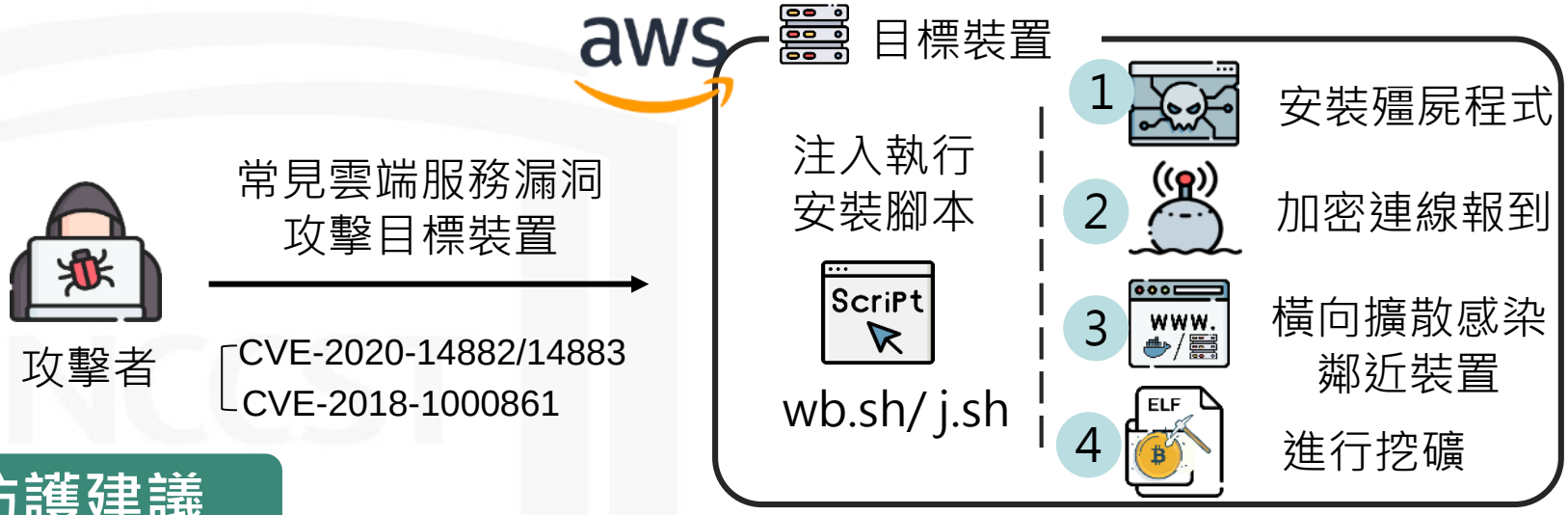


防護建議

- 提升機關內部同仁資安意識，請留意相關電子郵件，注意郵件來源之正確性，勿開啟不明來源信件之附檔以防遭植入惡意程式
- 建議針對雲端服務之存取行為建立控管機制，並定期檢視網路可疑連線，避免造成資安漏洞。

雲端服務遭攻擊利用案例

- 111年技服中心蜜罐偵測Kinsing殭屍網路針對雲端服務之攻擊，駭客企圖利用WebLogic與Jenkins漏洞，感染雲端裝置後對內部進行擴散，並用以挖取門羅幣

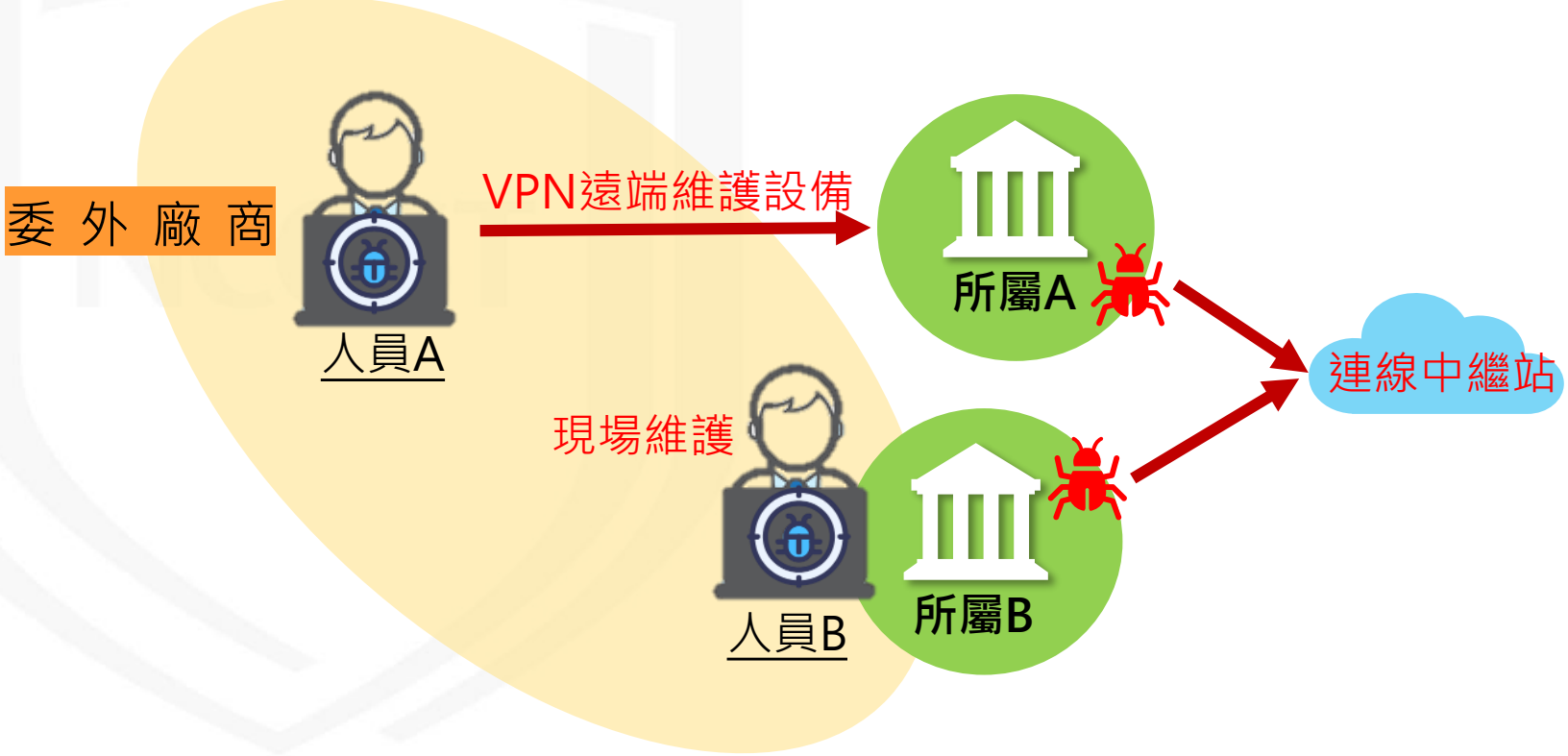


防護建議

- 以雲端平台建置對外服務之機關，應使用供應商最新公版容器建置服務，並定期更新軟體版本修補漏洞
- 建議針對雲端服務之存取行為建立控管機制，並定期檢視網路可疑連線，避免造成資安漏洞。

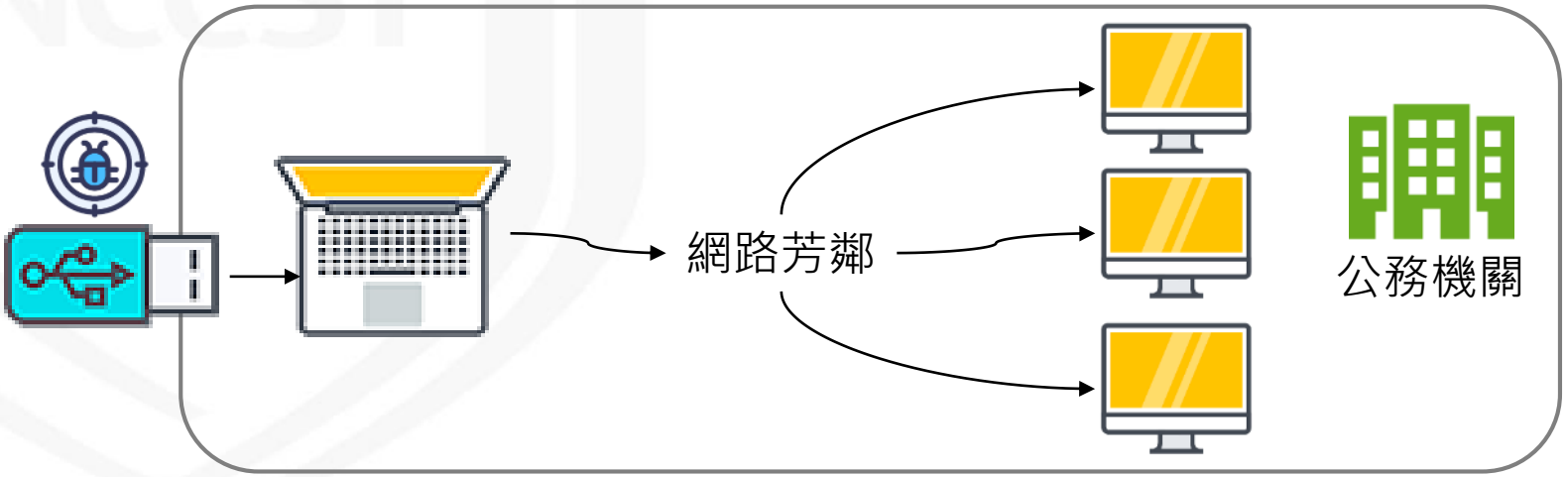
供應鏈攻擊-資訊廠商環境(1/3)

- 案例一：
  - 委外廠商人員電腦遭入侵植入惡意程式，廠商使用遭入侵之資訊設備維護機關資通系統，導致機關遭植入惡意程式
  - 委外廠商兩台電腦皆於相同資料夾路徑，發現相同的惡意程式，判斷該廠商內部存在資安風險



供應鏈攻擊-資訊廠商環境(2/3)

- 案例二：
  - 機關使用駐點廠商閒置電腦建置視訊環境，未先執行系統更新與安全檢測等作業，導致該電腦存在安全性漏洞遭利用，嘗試利用網路芳鄰協定對機關內部其他主機進行攻擊行為
- 案例三：
  - 廠商至機關進行電話交換機設定維護作業，將中毒USB插入機關提供之電腦並連網，連帶資訊設備中毒並嘗試利用網路芳鄰協定(Port 445)對其他主機進行可疑連線行為



供應鏈攻擊-資訊廠商環境(3/3)

防護建議

- 建議機關選任計畫委辦廠商時，依資通安全管理法與子法要求評估適當之受託者，並監督其資通安全維護情形
- 執行計畫時，機關應要求廠商建置環境之設備符合機關資安要求，並循正常流程管道申請使用機關設備，避免未經管制設備於機關環境中使用
- 作業執行前，機關或廠商應將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險

物聯網裝置應用風險案例

- 案例一：
  - 111年8月，因美國聯邦眾議院議長裴洛西訪台行程一事，導致台灣攻擊事件頻傳，超商與車站電子看板等物聯網設備遭駭客入侵並置換內容[19]

- 案例二：
  - 111年9月，經偵測發現某機關設備有異常連線行為，進一步確認時發現該機關受駭設備為門禁系統，且存在身分驗證繞過漏洞，駭客透過該漏洞入侵設備，並安裝惡意程式

防護建議

- 管理介面應強化存取控制
- 盤點機關內部相關IT與OT資產並納入風險評估
- 可透過VANS系統定期檢視相關IT與OT設備漏洞並更新

資料外洩/人為疏失案例

- 機關委託廠商辦理競賽活動，並提供活動資訊，欄位包含姓名與行動電話號碼等，廠商工作人員為協助活動宣傳，將參與人員資訊上傳至個人公開網站，造成個資資料外洩

防護建議

- 建議機關選任計畫委辦廠商時，合約中應納入資通安全管理法與個資法相關要求，並監督廠商落實執行
- 資料放置於網站前，應審核確實公告內容含有個資之必要性，不得逾越特定目的之必要範圍
- 資料上傳至公開網站後，應重複確認公開之資訊內容適切性
- 活動結束後，應監督廠商完成資料或相關存取權限等，返還、移交、刪除或銷毀，以及資料自網站下架

勒索病毒/人員資安意識

- 案例一：
  - 機關人員使用公務電腦瀏覽網站，點擊下載與執行偽裝成微軟更新包之惡意程式，大陸影音網即遭植入勒索病毒，並透過網路芳鄰感染網路硬碟，致個人電腦與網路硬碟檔案資料遭加密
- 案例二：
  - 機關人員個人電腦之檔案遭加密，經查為同仁於上班時段瀏覽免費漫畫網站，點擊惡意連結，下載並執行檔案，導致個人電腦感染勒索病毒

防護建議

- 加強內部同仁資安觀念：公務電腦應僅供公務使用
- 軟體更新作業應配合機關政策，並勿下載未經授權軟體

資料維護/網站資料維護

- 機關維護之網站提供外部A單位連結，由於A單位之舊網域租用到期未續約，後由其他公司註冊為色情網站
- 因機關未即時接獲相關消息並更新連結資料，以致使用者點擊該連結時導向至色情網站

防護建議

- 機關人員除定時檢視網站自身內容，亦應確保連結之正確性，避免導致民眾連結至錯誤之網站

設備管理不當/誤用報廢設備

- 某機關設備遭駭客暴力破解遠端桌面登入密碼進而植入惡意程式，由於該設備老舊並規劃報廢，故未進行處置
- 同仁誤使用該設備執行網路維護測試並連網，導致設備再次連線至駭客中繼站

防護建議

- 機關應訂定資訊設備報廢處理相關作業程序，並落實報廢設備管理規定，以避免待報廢設備衍生資安問題之疑慮
- 作業執行前，機關應確認設備已將作業系統與防毒軟體更新至最新版本，並持續更新修補漏洞，以降低遭外部入侵風險

大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

完善防護以因應資安威脅

- 機關應配合資通安全管理法，符合其所屬資通安全責任等級之要求，落實資通安全防護應辦事項，以因應六大類資通安全威脅情勢變化
  - 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
  - 針對郵件安全應備電子郵件過濾機制，並可加強郵件驗證機制與保留郵件日誌
  - 定期進行系統安全性檢測與資安健檢，包含弱點掃描與滲透測試，並完善資安弱點通報機制，以持續改善資安漏洞
  - 資通系統應進行風險評估分級，定期檢視是否符合防護基準，如委外開發、採購系統及雲端服務
  - 確保委外廠商與雲端服務業者執行受託業務時，遵循資通安全相關法令，並接受適任性查核
  - 避免採購或使用對國家資通安全具有直接或間接造成危害風險之系統或產品，如陸廠之物聯網設備與雲端服務

大綱

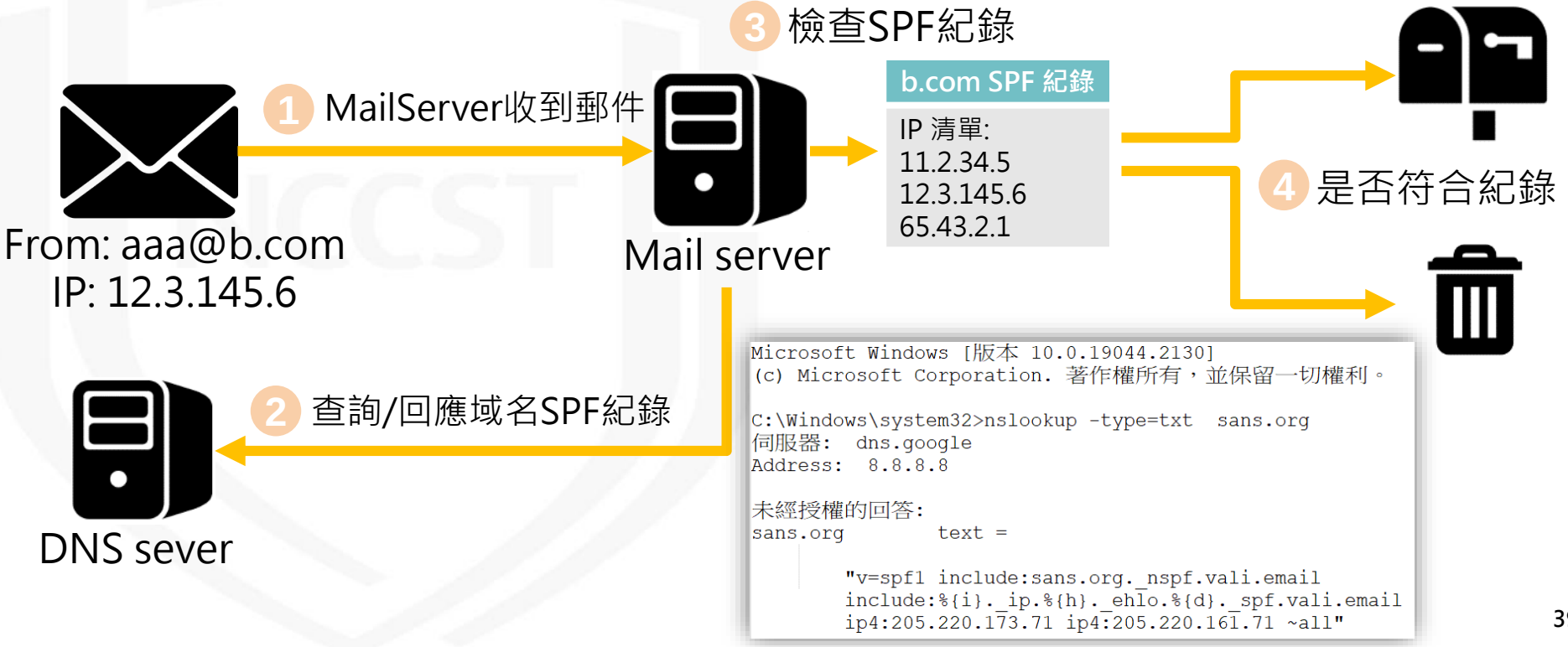
- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

強化郵件安全與防護整備(1/2)

- 密碼強度原則
  - 符合密碼強度，如大小寫、長度至少12碼及包含特殊符號等
- 密碼變更原則
  - 符合變更原則，如不同先前5次密碼，執行變更後留存相關紀錄
- 留存郵件日誌
  - 以利溯源異常登入行為IP位址，分析可能之入侵狀況，如是否存在密碼暴力嘗試登入與資訊外洩跡象

強化郵件安全與防護整備(2/2)

- 寄件者原則架構(Sender Policy Framework, SPF)
  - 使用DNS紀錄，指定寄件主機IP位置
  - 宣告機關自身寄送郵件來源正確性，提供其他機關檢驗
  - 檢驗收取郵件來源之伺服器IP位址，查核其他寄件來源



大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

落實資產管理與弱點修補

- 定期盤點資通系統資產
  - 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

- 即時修補資訊資產弱點
  - 接收VANS弱點通知
  - 即時進行漏洞修補與安全性更新
- 強化存取系統控制管理
  - 定期檢視可存取系統之帳號與IP列表，並確認存取權限
  - 定期更換密碼，並符合其密碼複雜度要求

大綱

- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例分享
- 政府機關資安防護強化重點
  - 完善防護以因應資安威脅
  - 強化郵件安全與防護整備
  - 落實資產管理與弱點修補
- 結論與建議

結論與建議(1/2)

- 機關應加強內部宣導，提升人員郵件資安意識，持續強化郵件安全與相關防護
  1. 業務負責窗口，應謹慎留意可疑電子郵件，注意郵件來源正確性，防範駭客利用電子郵件進行攻擊
  2. 郵件伺服器管理，透過DNS系統設定寄件者原則架構(SPF)，避免機關電子郵件帳號遭偽冒，進行社交工程攻擊
- 持續提升機關人員個人資安與機敏資料保護意識
  1. 公務電腦應避免從事非公務用途，勿下載其他軟體造成資安風險
  2. 落實個資「認知宣導及教育訓練」，蒐集個人資料以最少必要資訊為原則，資料若需上傳至公開網站，則應重複確認資料存取設定與保存之妥適性

結論與建議(2/2)

- 機關應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. 建置系統時避免未經管制設備於機關環境中使用
  2. 遠端維護資通訊設備系統應採「原則禁止、例外允許」方式
  3. 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
- 機關應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. 配合資通安全管理法要求，導入政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)
  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

報告完畢
敬請指教

參考資料(1/2)

[1] H2 2022: Threat Actors Impersonate 265 Different Brands in Credential Phishing Attacks, https://intelligence.abnormalsecurity.com/resources/h2-2022-report-brand-impersonation-phishing

[2] ZINC weaponizing open-source software, https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/

[3] In the footsteps of the Fancy Bear: PowerPoint mouse-over event abused to deliver Graphite implants, https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/

[4] Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets, https://www.recordedfuture.com/chinese-state-sponsored-group-ta413-adopts-new-capabilities-in-pursuit-of-tibetan-targets

[5] 2021 Top Routinely Exploited Vulnerabilities, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

[6] Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors, https://www.cisa.gov/uscert/ncas/alerts/aa22-279a

[7] Trend Micro 2022 Midyear Cybersecurity Report, https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report

[8] Supply Chain Security Gaps: A 2022 Global Research Report, https://www.isaca.org/resources/reports/supply-chain-security-gaps-a-2022-global-research-report

[9] DEV-0537 criminal actor targeting organizations for data exfiltration and destruction, https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/

參考資料(2/2)

[10] 深度剖析針對台灣金融業的 Operation Cache Panda 組織型供應鏈攻擊, https://medium.com/cycraft/supply-chain-attack-targeting-taiwan-financial-sector-bae2f0962934

[11] Nozomi Networks OT IoT Security Report, https://www.cisa.gov/uscert/sites/default/files/ICSJWG-Archive/QNL_SEP_22/Nozomi-Networks-OT-IoT-Security-Report-ES-2022-1H_508c.pdf

[12] 2022 Election Phishing Attacks Target Election Workers, https://www.trellix.com/en-us/about/newsroom/stories/research/2022-election-phishing-attacks-target-election-workers.html

[13] The most dangerous vulnerabilities exploited in 2022, https://resources.infosecinstitute.com/topic/most-dangerous-vulnerabilities-exploited/

[14] Fresh Phish: Small Business COVID-19 Grants Designed for Disaster, https://www.inky.com/en/blog/fresh-phish-small-business-covid-19-grants-designed-for-disaster

[15] Hackers Build Phishing Pages Using AWS Apps, https://www.avanan.com/blog/hackers-build-phishing-pages-using-aws-apps

[16] Updated Okta Statement on LAPSUS$, https://www.okta.com/blog/2022/03/updated-okta-statement-on-lapsus/

[17] 18 Most Popular IoT Devices In 2022 (Only Noteworthy IoT Products), https://www.softwaretestinghelp.com/iot-devices/

[18] Top IoT Security Threats in 2022, https://iotbusinessnews.com/2022/05/02/16441-top-iot-security-threats-in-2022/

[19] 台鐵也遭駭 新左營車站竟出現「老巫婆竄訪台灣」, https://udn.com/news/story/6656/6508637