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7月

大綱

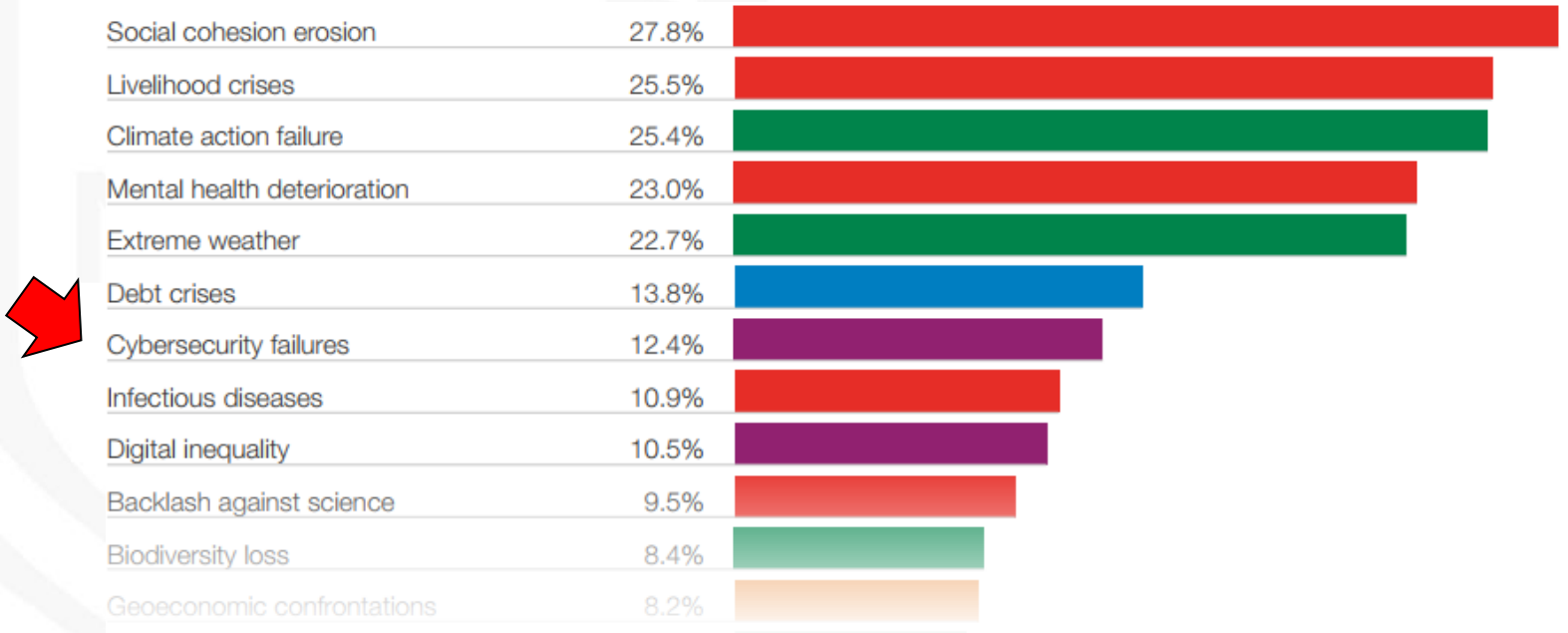
- 資安威脅趨勢與案例分享
  - 全球資安威脅趨勢
  - 政府資安威脅趨勢
  - 政府資安案例宣導
- 政府機關資安防護強化重點
  - 強化事前資安整備作業
  - 強化資安縱深防禦機制
- 結論與建議

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
  - 政府資安案例宣導
- 政府機關資安防護強化重點
  - 強化事前資安整備作業
  - 強化資安縱深防禦機制
- 結論與建議

世界經濟論壇2022全球風險調查報告

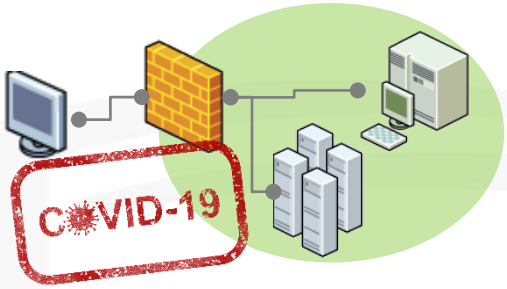
- 世界經濟論壇(World Economic Forum, WEF)發布之2022年全球風險報告[1]統計
  - 因新冠肺炎疫情對全球經濟、生活及技術應用等不同面向造成影響，有關經濟、環境、地緣政治、社會及科技等5大類風險中，其中科技類型風險以「網路安全失效(Cybersecurity failures)」最高



資料來源：[1]The Global Risks Report 2022 17th Edition, World Economic Forum

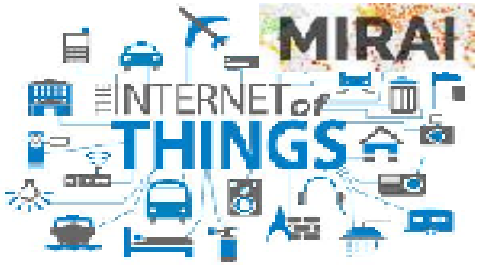
全球資安威脅趨勢

- 綜整2021年全球資安威脅與相關研究報告，歸納全球資安威脅趨勢



疫情造成
資安風險提高

勒索軟體攻擊
風險激增



IoT與行動式設備
資安弱點威脅升高

資安(訊)供應商持續遭
駭破壞供應鏈安全

APT鎖定式攻擊
竊取機密資料

社交工程詐騙盛行

資料來源：1.ENISA Threat Landscape 2021
2.ACSC Annual Cyber Threat Report
3.Microsoft Digital Defense Report
4.Fortinet Global Threat Landscape Report

疫情造成資安風險提高

- CyberEdge Group發表之「Cyberthreat Defense Report 2021」[1] 報告指出，新冠肺炎疫情後，全球企業實施居家辦公比例，由原本24%增加至50%
  - 工作型態之改變，對於遠端存取、應用及雲端等需求升高，導致資安邊界擴展，產生管理多面向之挑戰
- 駭客鎖定居家辦公之資安破口
  - 美國國土安全部網路安全暨基礎安全局(CISA)於2021年發布AA21-209A警訊，說明常被攻擊者利用之12個漏洞，超過半數為遠端工作環境所需之VPN連線或雲端技術相關漏洞

受影響廠商	遭利用之弱點
Citrix	CVE-2019-19781
Pulse	CVE 2019-11510
Fortinet	CVE 2018-13379
F5- Big IP	CVE 2020-5902
MobileIron	CVE 2020-15505
Microsoft	CVE-2017-11882
Atlassian	CVE-2019-11580
Drupal	CVE-2018-7600
Telerik	CVE 2019-18935
Microsoft	CVE-2019-0604
Microsoft	CVE-2020-0787
Microsoft	CVE-2020-1472

資料來源：[1] Cyberthreat Defense Report 2021 - CyberEdge Group
[2] Top Routinely Exploited Vulnerabilities, https://www.cisa.gov/uscert/ncas/alerts/aa21-209a , CISA, 2021

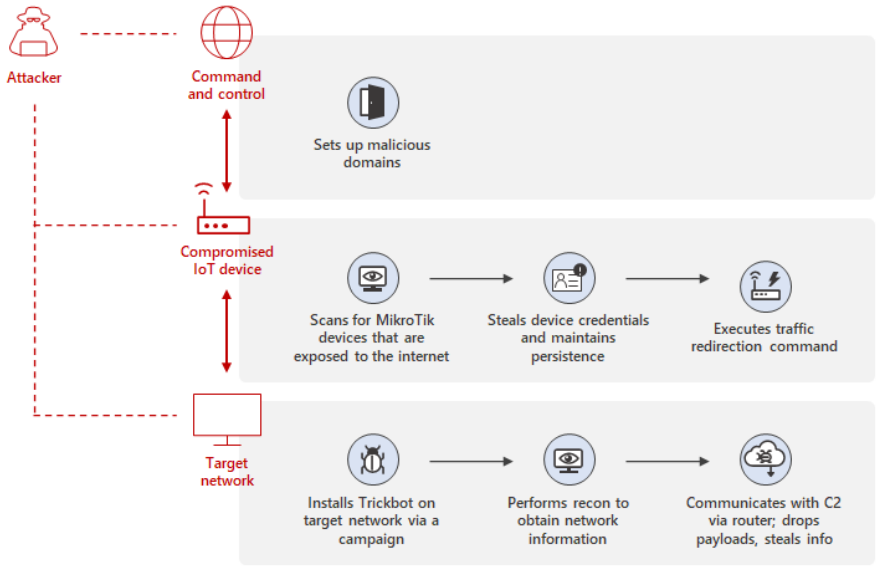
勒索軟體攻擊風險激增

- 日益增長之數位依賴加劇網路威脅
  - WEF「2021年全球風險報告」[1]指出，2020年惡意軟體與勒索軟體攻擊分別增加358%與435%
  - 勒索軟體即服務(Ransomware-as-a-Service, RaaS)之興起與網路犯罪生態體系之形成，推波助瀾下讓勒索軟體之威脅範圍與經濟損失日漸擴大
- 勒索軟體鎖定大型企業或政府關鍵基礎設施
  - Conti駭客集團對哥斯大黎加政府進行勒索軟體攻擊，導致含財務部、稅務及海關等機關資通系統停擺
  - Laspus$駭客集團攻擊全球包含T-Mobile、NVIDIA、微軟、三星等大型科技公司，致大量機密內容被公開

資料來源：[1]The Global Risks Report 2022 17th Edition, World Economic Forum

IoT與行動式設備資安弱點威脅升高

- IoT裝置常因老舊漏洞而被惡意程式攻擊，手機使用量增加導致手機木馬程式數量不斷增長
  - Check Point「2022 Cyber Security Report」[1]指出，攻擊者更廣泛使用網路釣魚簡訊來散播惡意軟體，藉此取得行動裝置之存取權限
  - TrickBot殭屍網路鎖定並入侵存在漏洞之MikroTik路由器，將其做為C2代理伺服器，透過非標準連接埠重導惡意流量，藉此規避偵測



Trickbot攻擊流程圖[2]

資料來源：[1]Check Point Software, 2022 Cyber Security Report
[2]Microsoft Security, Uncovering Trickbot's use of IoT devices in command-and-control infrastructure

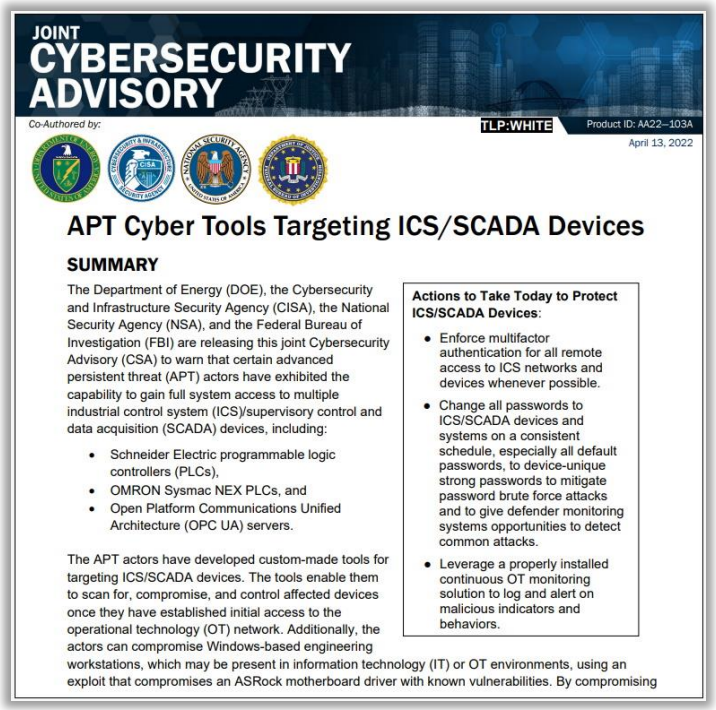
資安(訊)供應商遭駭破壞供應鏈安全

- 隨著對供應鏈之依存性越來越高，或是供應商數量越趨增加且其安全等級皆不相同時，亦意謂著供應鏈管控風險升高
  - 根據CyberGRX[1]調查報告顯示，超過53%之受訪者於過去2年曾經歷第三方資訊洩露事件，平均損失達750萬美元
  - 資安業者ESET於110年初揭露，知名Android遊戲模擬器NoxPlayer遭受供應鏈攻擊[2]，透過其更新機制植入惡意程式，蒐集包含用戶鍵盤輸入紀錄與機敏資訊等，受駭範圍包含台灣、香港及斯里蘭卡等

資料來源：[1]The Cost of Third-Party Cybersecurity Risk Management
[2]ESET uncovers Operation NightScout: Cyberespionage supply-chain attack on gamers in Asia

APT鎖定式攻擊竊取機密資料

- APT攻擊是常見網路攻擊手法，駭客集團常鎖定特定組織或國家，精心策劃結合多種攻擊手法，持續而隱匿地逐步滲透，藉此竊取機敏資料
  - 美國國土安全部網路安全暨基礎安全局(CISA)於2022年5月發布AA22-103A[1]警訊指出，已有APT駭客團體針對特定ICS/SCADA裝置，開發具備高度自動化攻擊能力之模組化工具，駭客成功進入OT網路後，即可透過工具掃描、入侵及操控受影響裝置



JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE Product ID: AA22-103A
April 13, 2022

APT Cyber Tools Targeting ICS/SCADA Devices

SUMMARY

The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising

Actions to Take Today to Protect ICS/SCADA Devices:

- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
- Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks.
- Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors.

資料來源：[1] APT Cyber Tools Targeting ICS/SCADA Devices, https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

社交工程詐騙盛行

- 社交工程電子郵件攻擊主要包含釣魚郵件與商業電子郵件詐騙
  - 趨勢科技「2021 Midyear Cybersecurity Report」[1]指出，犯罪活動大舉利用網路釣魚與社交工程詐騙，試圖利用政府防疫對策與各種管制訊息，將使用者導向與疫情相關之詐騙或假訊息網站
  - 微軟揭露駭客組織Nobelium[2]，藉由美國國際開發總署所使用之Constant Contact帳號，寄送惡意釣魚郵件至全球24個國家，逾150個組織之3,000個電子郵件帳號，鎖定並入侵供應商，再進一步攻擊供應商之客戶

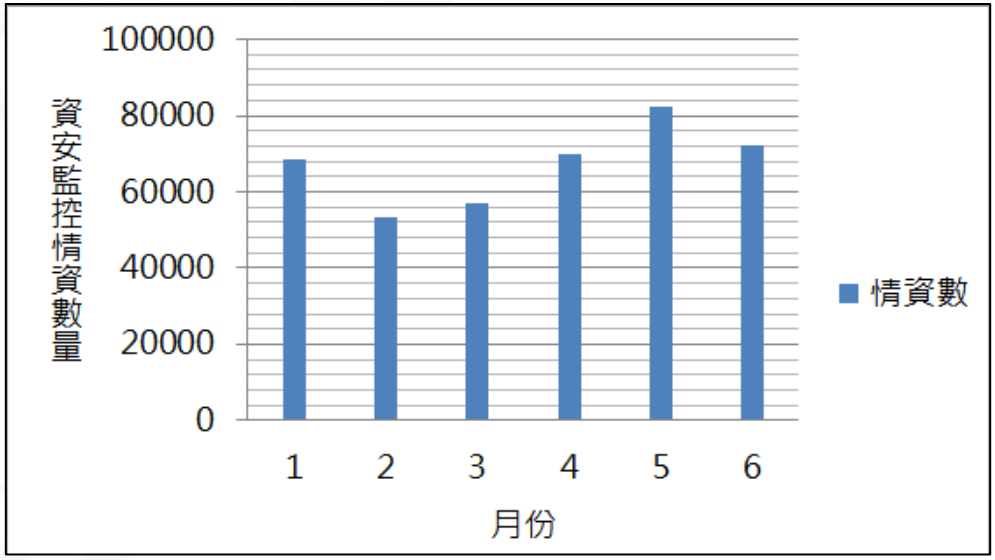
資料來源：[1]Attacks from all Angles: Trend Micro 2021 Midyear Cybersecurity Report, 2021
[2]New sophisticated email-based attack from NOBELIUM, Microsoft Security

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
  - 政府資安案例宣導
- 政府機關資安防護強化重點
  - 強化事前資安整備作業
  - 強化資安縱深防禦機制
- 結論與建議

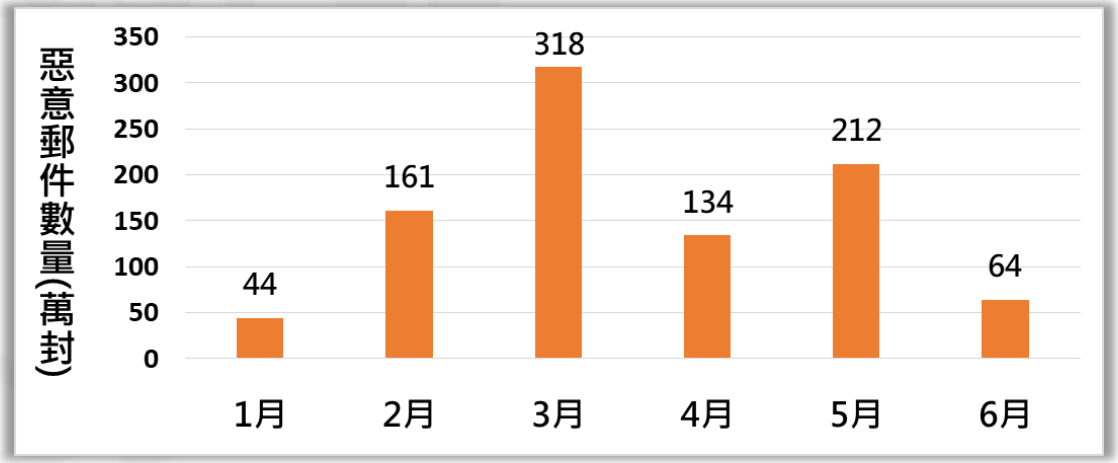
聯防監控情資威脅分析

- 111年上半年SOC業者回傳之有效資安監控情資數量共403,242件
  - 資安威脅種類排名前3名，分別為掃描刺探類(48%)、入侵攻擊類(28%)及政策規則類(13%)
  - 依政府機關業務類別排名前3名，分別為綜合行政類(33%)、外交國防法務類(22%)及非行政院所屬類(12%)



惡意電子郵件趨勢分析(1/2)

- 111年上半年政府領域社交工程釣魚郵件攻擊
  - 2月、3月及5月偵測到大量詐欺釣魚郵件散布，皆以取得收件人電腦機敏資訊或掌握使用者不堪影片為由，向受駭者勒索比特幣
- 111年上半年政府領域惡意程式垃圾郵件攻擊
  - 自2月底起至今，發現Emotet惡意垃圾郵件開始大量散布，並使用社交工程手法以增加成功率

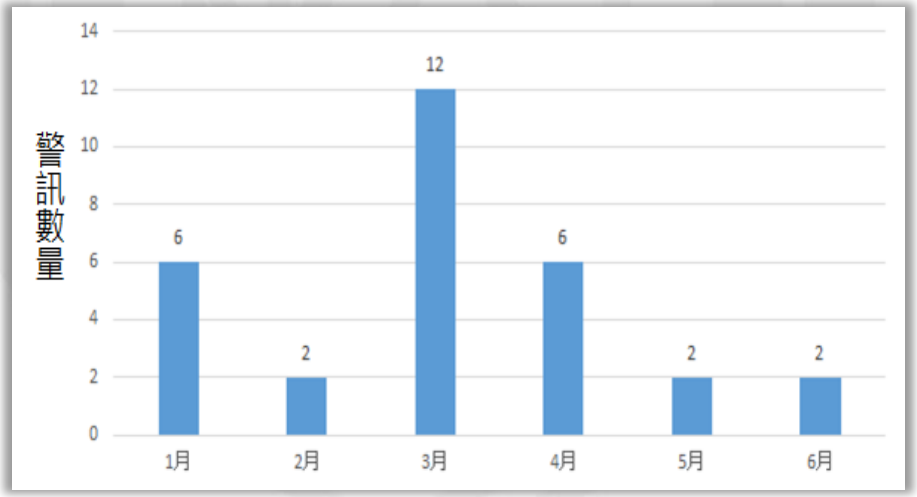


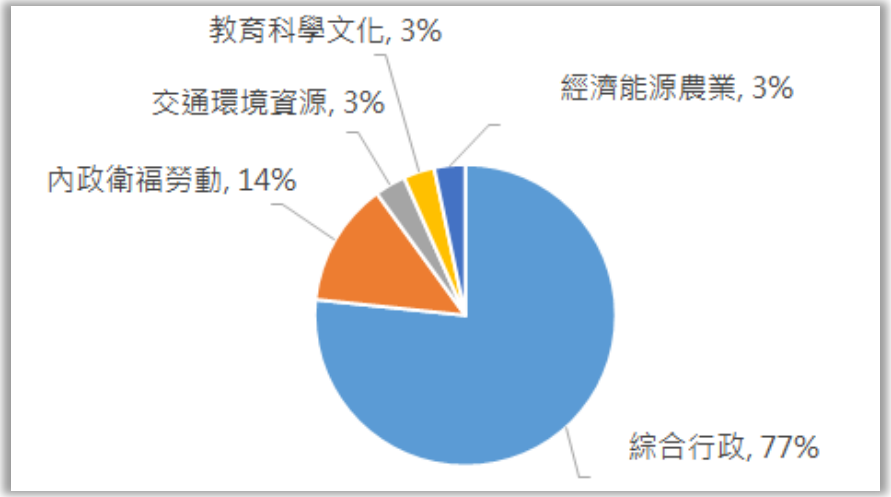
惡意電子郵件趨勢分析(2/2)

- 111年上半年政府領域APT惡意電子郵件攻擊
  - 使用技巧命名(Right To Left Override, RTLO)攻擊，透過改變檔案名稱顯示方式，誘騙使用者開啟惡意郵件附檔，並利用公務相關主旨，針對特定人士發動魚叉式社交工程攻擊
  - 利用COVID-19疫情主旨，針對特定地區之政府機關與國中小學教職員發動社交工程電子郵件攻擊
- 111年上半年郵件附檔惡意程式弱點利用
  - CVE-2017-11882為微軟Office系列之遠端執行漏洞，適用平台廣泛且容易被觸發，自106年被發現至今仍是駭客最常利用之漏洞

挖礦劫持威脅分析

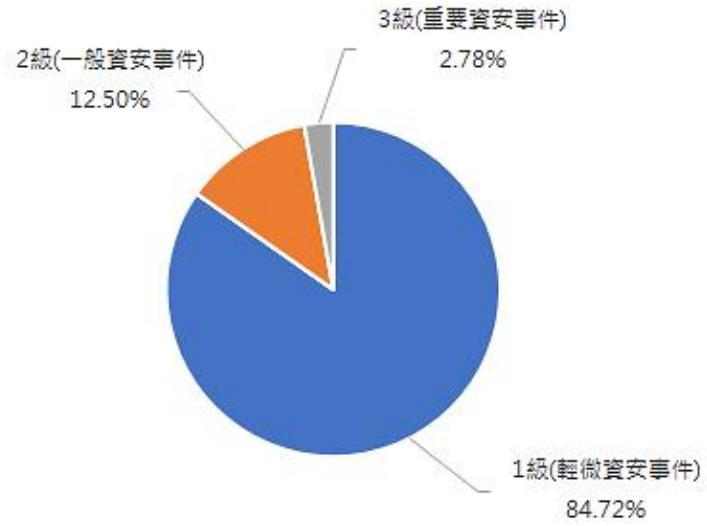
- 111年上半年偵測到政府機關所屬設備連線至礦池，並存在報到之異常行為，共發布30則資安警訊通知機關進行應變處置
  - 以綜合行政類機關遭駭侵最為嚴重(77%)
  - 可明確判斷發生原因之事件，以系統弱點與使用者安裝非授權之軟體為主

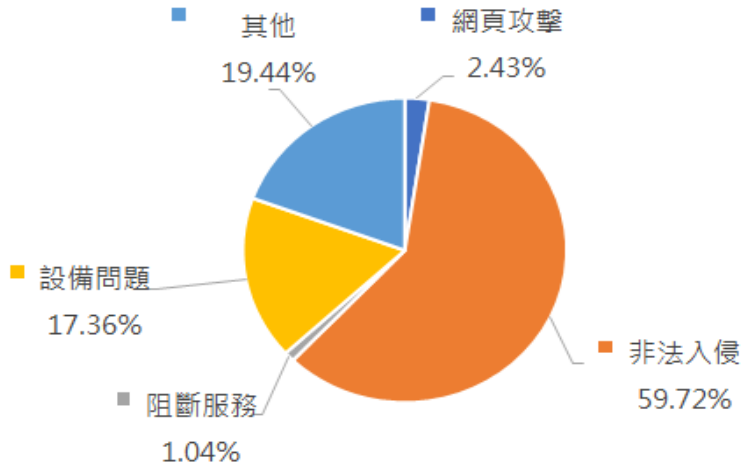




通報事件分析(1/2)

- 111年上半年共接獲288件資安事件通報
  - 事件影響等級以1級事件為主
  - 通報類型比例分析
    - 以非法入侵類型為大宗，占58.85%，部分事件原因為供應鏈廠商或產品遭到攻擊所致
    - 其餘事件可明確分類者，以設備問題與網頁攻擊為主
  - 44.44%(145件)為機關接獲技服中心警訊通報後所進行之通報





通報事件分析(2/2)

- 111年截至6月30日，3級資安事件通報共8件

造成影響	發生原因
資料外洩	■ 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
資料或系統異常	■ 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

111年政府資安威脅趨勢

政府機關資通安全威脅趨勢

- **供應鏈攻擊**，攻擊者鎖定供應鏈廠商發動攻擊，提升攻擊效益
- 人員資安意識不足，導致**資料外洩事件**持續發生
- 設備弱點未即時更新，致遭利用發動**挖礦劫持**
- **社交工程郵件**仍為常見攻擊手法

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
  - 政府資安案例宣導
- 政府機關資安防護強化重點
  - 強化事前資安整備作業
  - 強化資安縱深防禦機制
- 結論與建議

資安事件常見態樣

供應鏈攻擊

- **廠商環境**：廠商遭入侵並將做為跳板，進一步駭侵機關
- **產品漏洞**：產品設計不當或零時差漏洞(ZeroDay)利用

資料外洩

- **作業疏失**：行政作業疏失，將機敏資料上傳至公開平台
- **設定不當**：對系統操作不熟悉，致使檢視權限設定不當

挖礦劫持

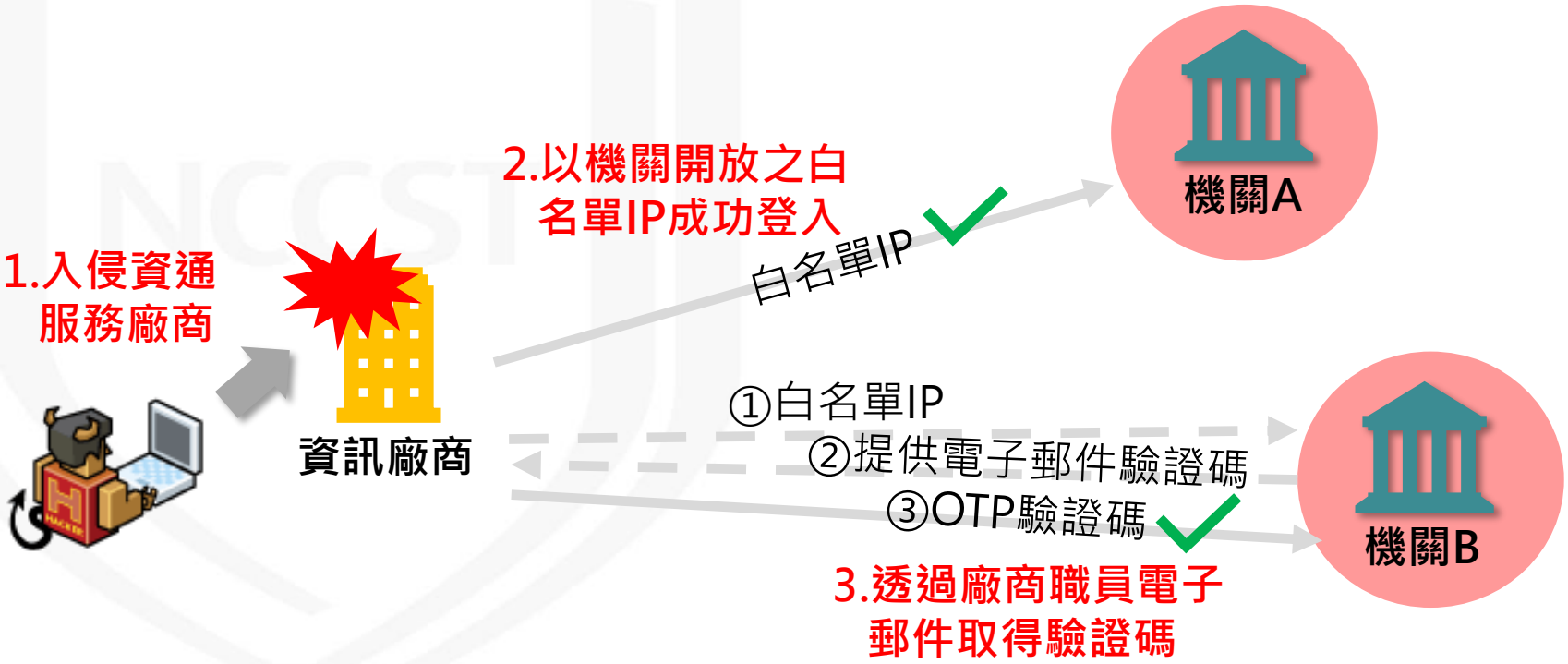
- **產品漏洞**：產品資安漏洞遭利用，濫用受駭設備資源採礦
- **管理疏失**：安裝未經授權程式，缺乏日誌紀錄保存機制

惡意郵件

- **人員意識**：人員資安意識不足，誤開啟郵件
- **系統弱點**：系統弱點未即時修補，致使遭利用入侵

供應鏈攻擊-資訊廠商環境(1/2)

- 駭客利用資安漏洞入侵資通服務廠商內部環境，並取得其可遠端登入服務之客戶帳號密碼
- 多個政府機關皆遭同一來源IP入侵成功
  - 部分機關採用郵件作為多因子驗證方式之一，因該廠商內部環境已遭入侵，故駭客仍可成功入侵機關



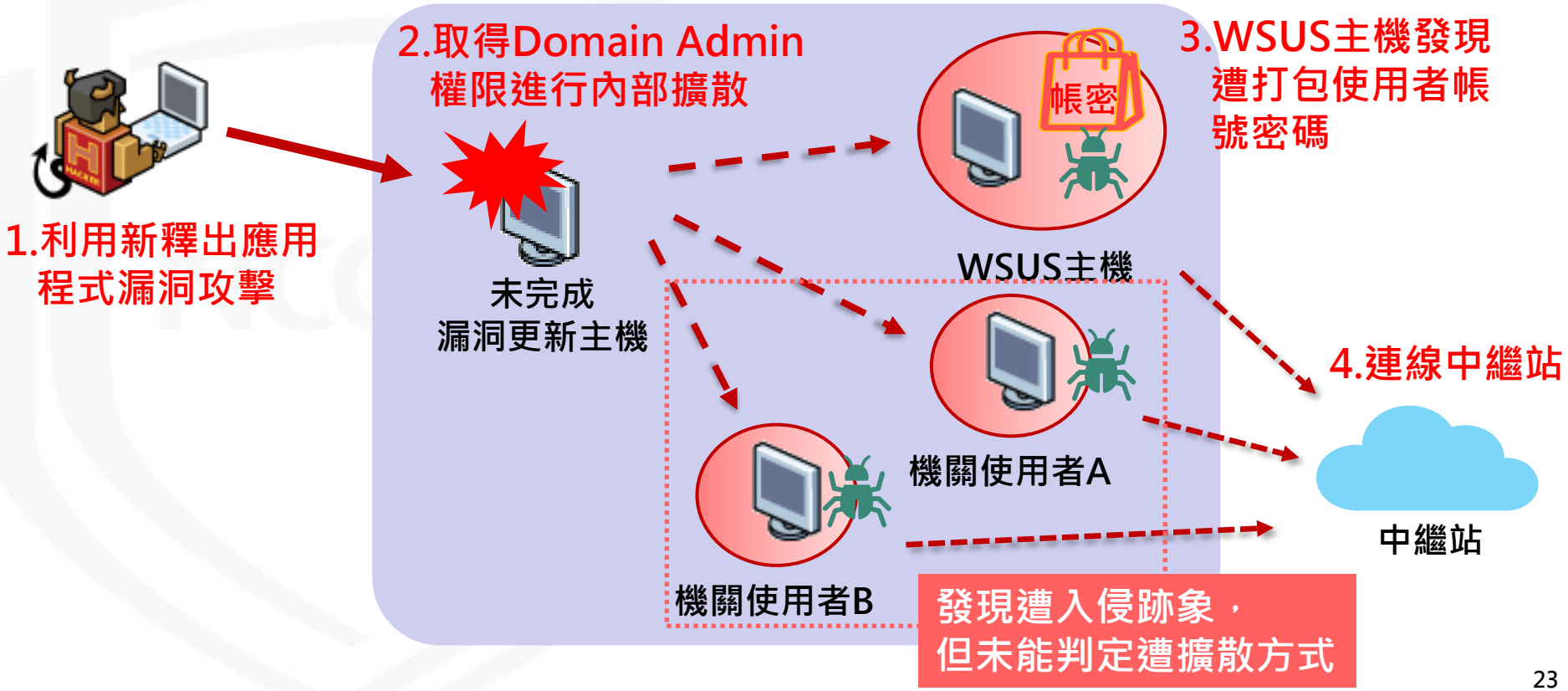
供應鏈攻擊-資訊廠商環境(2/2)

防護建議

- 遠端維護資通系統應採「原則禁止、例外允許」方式
  - 行政院資通安全處 110 年 3 月 2 日院臺護字第 1100165761 號函
- 開放遠端存取期間原則以短天期為限，並建立異常行為管理機制
  - 可採多因子驗證方式，加強遠端登入身分驗證
  - 稽核帳號登入時間與執行紀錄，以確認時間與作業項目皆與實際情況相符
- 結束遠端存取後，確實關閉網路連線，並更換遠端存取通道(如VPN)之登入密碼等

供應鏈攻擊-應用程式漏洞(1/2)

- 駭客利用更新應用程式漏洞時間差，成功入侵機關設備
- 由於該主機由Domain Admin權限帳號建立，因此成功入侵後即可進行內部擴散



供應鏈攻擊-應用程式漏洞(2/2)

防護建議

- 應留意內部使用之資通系統更新資訊
- 接獲漏洞更新訊息，應儘速檢視資通系統版本等資訊，並安排系統更新時程
- 檢視系統相關紀錄檔，確認尚未遭駭客利用漏洞入侵成功

資料外洩-人為疏失

- 機關辦理研討活動並請參與人員報到，表單欄位包含姓名、身分證字號及手機
- 承辦人員未檢視上傳資料內容，將活動成果資訊上傳至公開網站，造成個資外洩

防護建議

- 如需蒐集個人資料，以最少必要資訊為原則
- 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
- 若活動採取線上報名方式，承辦人員確認蒐集資料內容，測試資料蒐集與相關作業流程
- 持續加強機關人員個人資料保護意識

資料外洩-社交工程

- 某機關透過臉書(Facebook)粉絲專頁宣導活動資訊，並利用Message接收報名資訊
- 粉絲專頁管理員疑似遭社交工程攻擊成功，導致帳號密碼外洩，進而造成民眾個資存在外洩疑慮

防護建議

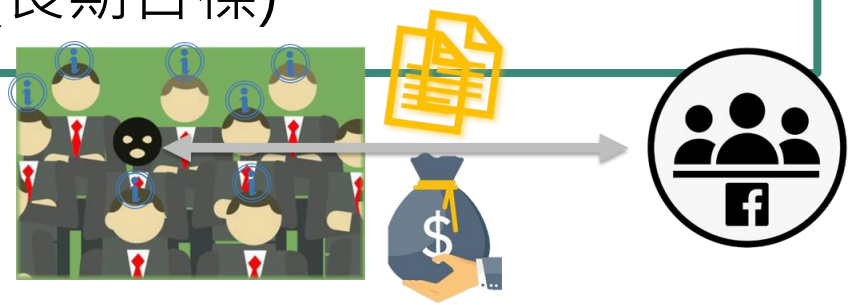
- 經營公務用途之社群應妥善管理帳號，相關人員亦應提高資安意識
- 避免利用網路公開平台蒐集敏感資料，若因活動需求，則應重複確認資料存取設定與保存之妥適性
- 持續加強機關人員資安防護與個資保護意識

資料外洩-設定錯誤

- 某機關接獲民眾檢舉，於社交平台發現有人兜售該機關保管之個人資料
- 經調查發現為離職員工濫用系統存取權限，擅自下載機關所持有的民眾個資並進行兜售

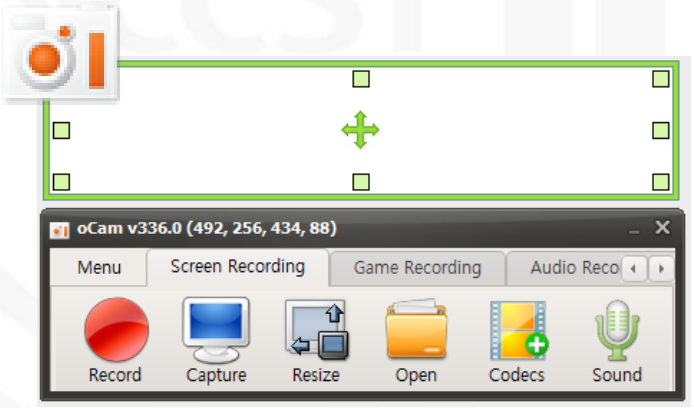
防護建議

- 定期清查系統帳號使用情況
- 應將審查系統帳號刪除(停用)作業納入離職流程
- 落實個資「認知宣導及教育訓練」
- 將資通系統調整零信任架構(長期目標)



挖礦劫持(1/3)

- 挖礦劫持指未經使用者同意或知悉之情況下，劫持系統資源執行挖礦程式
  - 超過15個機關受駭主機皆連往相同礦池，分析後發現，皆安裝免費螢幕錄影軟體oCam，惟舊版軟體預設會安裝BRTSvc(Blockchain Research Tools)，並使用系統資源進行挖礦以做為贊助用途，使用者需在軟體安裝過程中自行取消安裝該服務(新版改為付費軟體，暫無發現相同問題)



挖礦劫持(2/3)

- NAS類型產品易成為駭客鎖定目標，主要透過系統漏洞進行入侵，造成之影響包含設備資料遭勒索加密、使用系統資源進行挖礦及造成資料毀損
  - 偵測到5個機關NAS設備，遭植入惡意程式(UnityMiner)進行挖礦劫持(皆利用QNAP之Helpdesk應用程式漏洞)
  - 惡意程式會置換系統檔案managRequest.cgi(功能為檢查目前設備處理器使用率)來竄改系統數據，使用者將無法從系統管理工具中直接觀察到設備CPU使用率異常，藉此隱匿挖礦劫持行為

漏洞編號	說明
CVE-2020-2506	權限控制漏洞，可讓攻擊者取得QNAP NAS設備的控制權限
CVE-2020-2507	指令注入漏洞，可讓攻擊者遠端執行任意程式碼

挖礦劫持(3/3)

- 部分資通訊設備受限於設備資源，日誌紀錄不完整，較難進一步追查入侵原因
- 依111年4月Check Point發表之全球威脅指數，被用來進行挖礦劫持之門羅幣開源挖礦軟體(XMRig)依然榜上有名

Global Threat Index - Top 10 Malware			
排名	惡意程式	排名	惡意程式
1	Emotet	6	Lokibot
2	Formbook	7	Ramnit
3	Agent Tesla	8	Phorpiex
4	XMRig	9	Mirai
5	Glupteba	10	Remcos

防護建議

- 加強防範社交工程攻擊
- 定期修補系統漏洞與更新防毒軟體病毒碼
- 避免私自安裝未經核可或非公務需求之應用程式
- 網路閘道端封鎖惡意網址(礦池域名)
- 強化相關日誌紀錄保存與管理，以利事件根因分析

資料來源：[1]Check Point Research, April 2022's Most Wanted Malware

惡意電郵攻擊

- 111年Emotet惡意垃圾郵件遽增，攻擊與感染手法多變，透過不同混淆機制以規避防毒掃描偵測，並利用姓名、職稱及曾往來郵件主旨等做為郵件主旨，引誘收件人開啟郵件

Emotet惡意附檔演變

No.	郵件主旨範例
1	陳OO
2	Re:陳主任OO
3	RE: 陳OO(人事室)
4	Fwd:陳OO
5	Fwd:
6	RE:
7	[空白主旨]
8	Re: XXXX局的結案資料

防護建議

- 注意郵件來源之正確性，勿開啟不明來源之郵件附檔
- 建立網路服務之存取行為控管機制，並定期檢視網路可疑連線
- 關閉Office系列之自動啟用巨集功能

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
  - 政府資安案例宣導
- 政府機關資安防護強化重點
  - 強化事前資安整備作業
  - 強化資安縱深防禦機制
- 結論與建議

強化事前資安整備作業(1/2)

- 即時漏洞修補
  - 隨時注意重大漏洞訊息，即時修補防護
  - 上線系統定期執行滲透測試與弱點掃描，及早發覺潛在漏洞
  - 導入資通安全弱點通報機制(Vulnerability Alert and Notification System, VANS)，掌握整體風險情勢，並落實資產盤點與弱點管理

強化事前資安整備作業(2/2)

- 強化人員資安意識
  - 避免開啟非公務相關郵件，降低社交工程攻擊威脅
  - 避免因人員意識不足，權限設定錯誤而導致機敏資料外洩
- 落實系統紀錄保存
  - 妥善規劃保存系統紀錄，以利資安事件鑑識分析
  - 系統紀錄應包含應用程式與作業系統等日誌紀錄，以利分析事件根因，改善資安管理

資通安全責任等級	保存範圍	保存項目
A	機關應保存全部資通系統與各項資通**及**防護設備最近六個月之日誌紀錄	• 作業系統日誌(OS event log) • 網站日誌(Web log) • 應用程式日誌(AP log) • 登入日誌(Logon log)
B	機關應保存全部核心資通系統與**相連**之資通及防護設備最近六個月之日誌紀錄	
C	機關應保存全部核心資通系統最近六個月之日誌紀錄	

參考來源：行政院「各機關資通安全事件通報及應變處理作業程序」

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
  - 政府資安案例宣導
- 政府機關資安防護強化重點
  - 強化事前資安整備作業
  - 強化資安縱深防禦機制
- 結論與建議

強化資安縱深防禦機制(1/3)

- 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，同時配合異常紀錄檢視，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

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

- 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

強化資安縱深防禦機制(2/3)

- 落實黑名單部署
  - 於防火牆等資安防護設備定期更新黑名單，以技服中心提供黑名單為基礎，增列機關自有防護規則，確保資安防護即時有效

黑名單下載方式

- 登入通報網站，在資安訊息公告之重要公告事項
- 每週四之公告事項，會提供完整版惡意中繼站清單(其餘日期公告事項內容僅註記增加/刪除之DN/IP)

強化資安縱深防禦機制(3/3)

- 導入端點偵測及應變機制
  - 配合資安法應辦事項要求，A、B級公務機關需將EDR偵測資料納入監控範圍，並依格式透過現有聯防監控資料回傳管道提交至主管機關
  - 透過端點偵測結果，強化事件關聯分析，掌握潛在攻擊來源

結論與建議(1/2)

- 機關應落實委外管理機制，並責成委外廠商遵守資安管理措施
  - 遠端維護資通系統應採「原則禁止、例外允許」方式
  - 如須開放遠端存取原則以短天期為限，並建立異常行為管理機制，以確認時間與作業項目皆與實際情況相符
- 持續加強機關人員個人資安與機敏資料保護意識
  - 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)

- 注意重大漏洞訊息，即時進行更新修補
  - 應隨時關注資通訊設備漏洞更新情況，並儘速完成漏洞修補作業
  - 如因機關環境未能即時完成漏洞更新，系統應暫時下線，關閉存在漏洞功能並加強監控機制
- 落實日誌保存
  - 參考「各機關資通安全事件通報及應變處理作業程序」要求事項，完善跡證保存，以利進行事件根因分析

報告完畢
敬請指教