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

110年

【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
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 提升主動防禦能量
  - 強化通報應變機制
- 結論與建議

世界經濟論壇2021全球風險調查報告

高↑風險發生影響性

風險發生可能性➔高

10大影響風險

1.傳染病
2.緩解氣侯變化行動失敗
3.大規模殺傷性武器
4.生物多樣式喪失
5.自然資源危機
6.人為環境災害
7.民生危機
8.極端氣侯
9.債務危機
10.資訊基礎建設破壞(109年排名第6)

10大可能長期風險

1.極端氣侯
2.緩解氣侯變化行動失敗
3.人為導致的環境災害
4.傳染病
5.生物多樣式喪失
6.數位集權
7.數位不平等
8.國際關係裂痕
9.資安防護失敗
10.民生危機

紅色：科技因素
藍色：2021年新增因子

資料來源：The Global Risks Report 2021 16th Edition, World Economic Forum

110年上半年全球資安事件(1/2)

1月

110年1月
美國軟體供應商Accellion文件傳輸系統FTA，存在安全性漏洞，致使用該系統之客戶資料外洩

#資料外洩 #供應鏈安全

2月

110年2月
加拿大飛機製造商龐巴迪，使用Accellion檔案傳輸服務，該服務存在漏洞遭到利用，導致資料外洩

#資料外洩 #供應鏈安全

110年2月
駭客入侵佛羅里達州供水系統，並試圖將氫氧化鈉含量增加到對人具有潛在危險

#關鍵基礎設施 OT

3月

110年3月
教育慈善機構哈里斯聯合會，遭勒索軟體攻擊，迫使該機構關閉IT系統，並暫時禁用電子郵件系統與總機服務，約影響36,000多名學生

#勒索軟體

110年3月
- 利用Exchange Server零時差漏洞進行大規模網路攻擊，美國有9個政府機構與60,000多家私人企業受到影響
- 超過10個APT組織，利用Microsoft Exchange漏洞進行攻擊

#APT

110年上半年全球資安事件(2/2)

3月

110年3月
宏碁公司遭遇勒索軟體攻擊，要求支付5,000萬美元贖金，創下迄今最高已知贖金紀錄

#勒索軟體

110年3月
IoT解決方案供應商Sierra Wireless，因遭到勒索軟體攻擊而暫時停產，導致該公司於1週後才恢復生產

#勒索軟體

110年3月
監控系統廠商Verkada遭到駭客入侵，駭客可存取該公司部署於客戶端之15萬台監視器即時畫面

#IOT安全 #資料外洩 #供應鏈安全

4月

5月

110年5月
美國CNA Financial最大網路保險公司，遭到新版本Phoenix CryptoLocker勒索軟體攻擊，被迫關閉3天

#勒索軟體

110年5月
美國最大的燃料管道系統商Colonial Pipeline遭駭客攻擊，支付約440萬美元(約新台幣1.23億)贖金

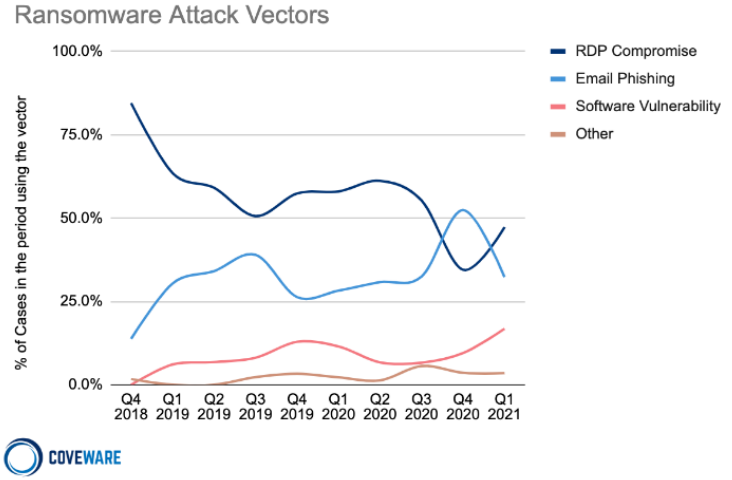
#勒索軟體 #關鍵基礎設施 OT

個人資料外洩攻擊白熱化

- 駭客攻擊為資料外洩主要原因
  - 美國身分竊盜資源中心(ITRC)資料外洩報告
    - 110年第1季資料外洩與109年相比增加12%
    - 網路釣魚與勒索軟體是資料外洩主因
- 駭客挾持機敏資料進行勒索
  - Clop利用Accellion FTA漏洞，竊取多家企業機敏資料，要求支付贖金否則就要公布受駭者機密資訊

勒索軟體攻擊風險激增

- 勒索軟體攻擊伴隨竊取機敏資料
  - 資安業者Coveware指出，勒索軟體攻擊涉及資料外洩威脅，相較於109年第4季70%增加到110年第1季77%
  - 遠端桌面協定(RDP)與惡意電子郵件為常見攻擊管道
- 勒索軟體攻擊平台轉移
  - 勒索軟體Babuk、Nephilim及Darkside轉向Unix與Linux平台
- VPN漏洞成入侵途徑
  - 資安業者Coveware發現，110年第1季常見遭利用之軟體漏洞涉及VPN設備，如Fortinet與Pulse Secure等



資料來源：
https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

IoT與行動式設備資安弱點威脅升高

- 網路資安廠商Fortinet台灣資安威脅趨勢報告
  - 台灣遭到超過200萬次攻擊與中國駭客有關，以針對物聯網設備(IoT)的殭屍網路(botnet)攻擊為主
- Mirai與Gafgyt仍活耀於物聯網殭屍網路，針對網路設備與IoT設備漏洞發動攻擊
  - Palo Alto於110年2月揭露新的Mirai殭屍網路變種病毒
  - Gafgyt使用Tor網路隱藏命令與控制行為
- Telnet弱密碼、SSH暴力破解及應用程式漏洞為常見入侵手法

受影響設備	遭利用之漏洞
D-Link	CVE-2019-16920 CVE-2020-25506
Citrix	CVE-2019-19781
Netgear ProSAFE Plus	CVE-2020-26919
Liferay Portal	RCE(無CVE編號)
SonicWall SSL-VPN	命令注入漏洞(無CVE編號)

※110年第1季Mirai與Gafgyt利用之漏洞

APT鎖定式攻擊竊取機密資料

- APT係有組織且具目的性的長期潛伏攻擊活動
  - 多個APT組織鎖定美國國防產業Pulse Connect Secure VPN漏洞進行攻擊，推測攻擊目標主要為美國國防工業基地
- 網路設備遭APT組織鎖定
  - 美國聯邦調查局110年3月指出，發現APT組織透過FortiGates設備漏洞，成功入侵美國地方政府網路
    - CVE-2018-13379
    - CVE-2019-5591
    - CVE-2020-12812

資料來源：https://cyber.dhs.gov/ed/21-03/

資料來源：https://www.ic3.gov/Media/News/2021/210527.pdf

資安(訊)供應商遭駭破壞供應鏈安全

- 供應鏈攻擊
  - 以軟(韌)體開發公司或委外人員做為跳板，利用受信任管道滲透客戶網路
  - 透過入侵特定軟(韌)體開發公司或委外人員電腦，進行程式竄改或下載連結等惡意行為
- 供應鏈攻擊透過單點攻擊入侵多個組織
  - SolarWinds事件導致約18,000個客戶安裝帶有惡意程式Orion更新軟體
  - 美國軟體供應商Accellion公告，因文件傳輸系統FTA存在安全性漏洞，約50個客戶受到影響


Cybercrime , Cyberwarfare / Nation-State Attacks , Fraud Management & Cybercrime

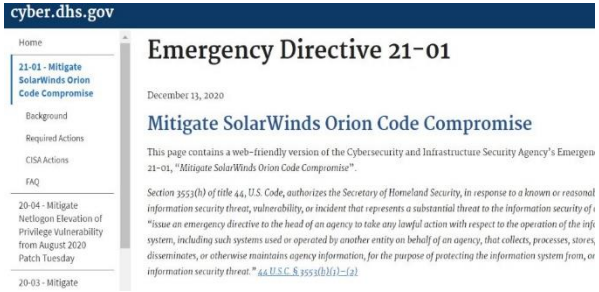
Cloud Hopper: Major Cloud Services Victims Named

Reuters Says Fujitsu, Tata, NTT Data, Dimension Data, CSC and DXC Affected

Jeremy Kirk (jeremy_kirk) • June 27, 2019

Twitter Facebook LinkedIn Credit Eligible Get Permission

資料來源：
https://www.bankinfosecurity.com/cloud-hopper-major-cloud-services-victims-named-a-12695


cyber.dhs.gov

Home

21-01 - Mitigate SolarWinds Orion Code Compromise

Background

Required Actions

CISA Actions

FAQ

20-04 - Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday

20-03 - Mitigate

Emergency Directive 21-01

December 13, 2020

Mitigate SolarWinds Orion Code Compromise

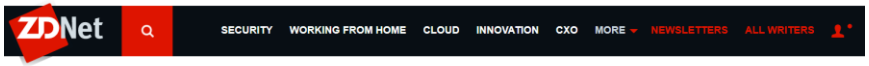
This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergen 21-01, "*Mitigate SolarWinds Orion Code Compromise*".

Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonal information security threat, vulnerability, or incident that represents a substantial threat to the information security of "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the inf system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, o information security threat." 44 U.S.C. § 3553(b)(2)–(3)

美國國土安全部要求
所有聯邦機構網站
關閉SolarWinds相關產品

關鍵基礎設施OT資安風險倍增

- IT領域與OT領域界限模糊增加資安風險
  - 110年2月，駭客利用淨水廠日常作業所使用TeamViewer漏洞存取工業控制系統，並更改淨水廠控制系統相關參數至超標數值



Following Oldsmar attack, FBI warns about using TeamViewer and Windows 7

An FBI alert sent on Tuesday warns companies about the use of out-of-date Windows 7 systems, poor account passwords, and desktop sharing software TeamViewer.

資料來源：https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/

- 勒索軟體攻擊造成OT營運威脅
  - 110年5月，美國最大燃油輸油管線Colonial Pipeline遭勒索軟體攻擊，雖僅影響IT系統，惟為防止進一步攻擊關閉OT營運，減少供油45%

BRIEF

Colonial Pipeline disconnects OT systems to silo ransomware IT threat

Published May 12, 2021

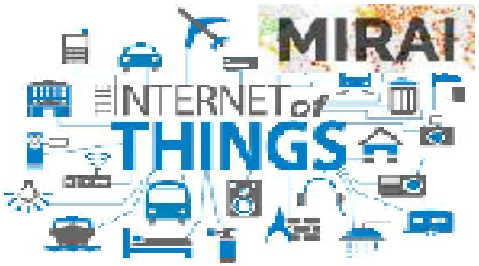
By David Jones
Reporter

資料來源：
https://www.cybersecuritydive.com/news/colonial-pipeline-OT-IT-ransomware/600046/

全球資通安全威脅趨勢綜合歸納

個人資料外洩
攻擊白熱化

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

APT鎖定式攻擊
竊取機密資料

資安(訊)供應商持續遭
駭破壞供應鏈安全

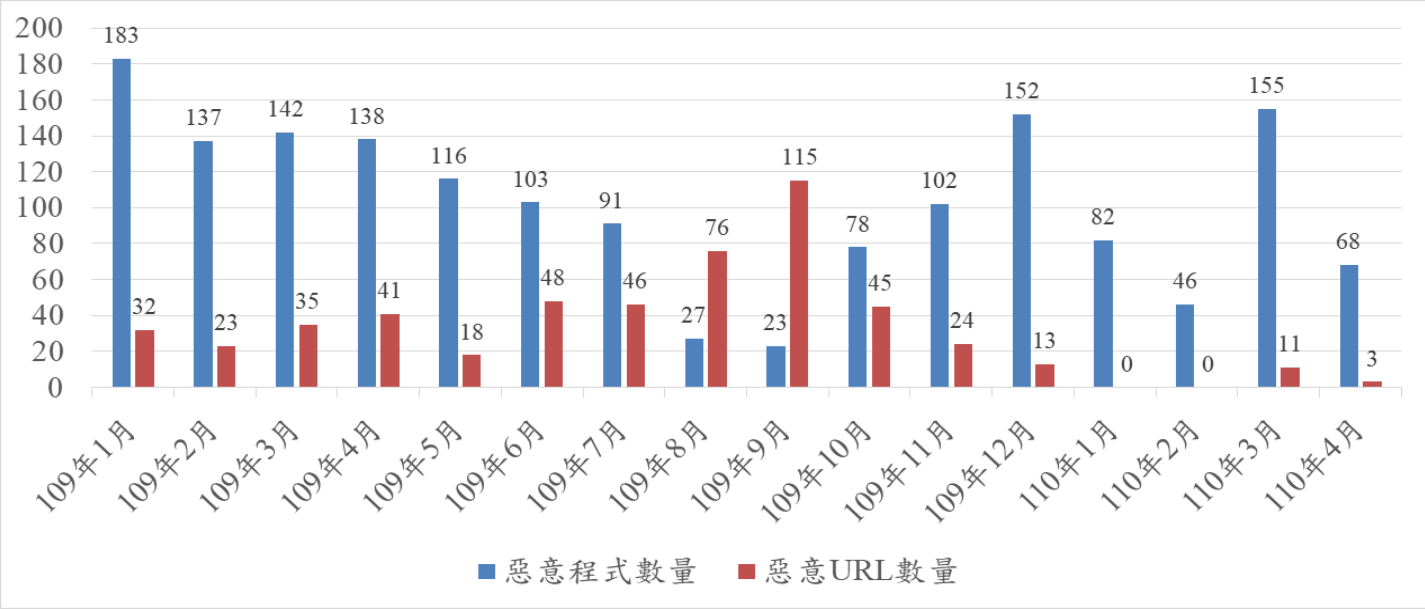
關鍵基礎設施OT
資安風險倍增

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
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 提升主動防禦能量
  - 符合法規要求強化通報應變機制
- 結論與建議

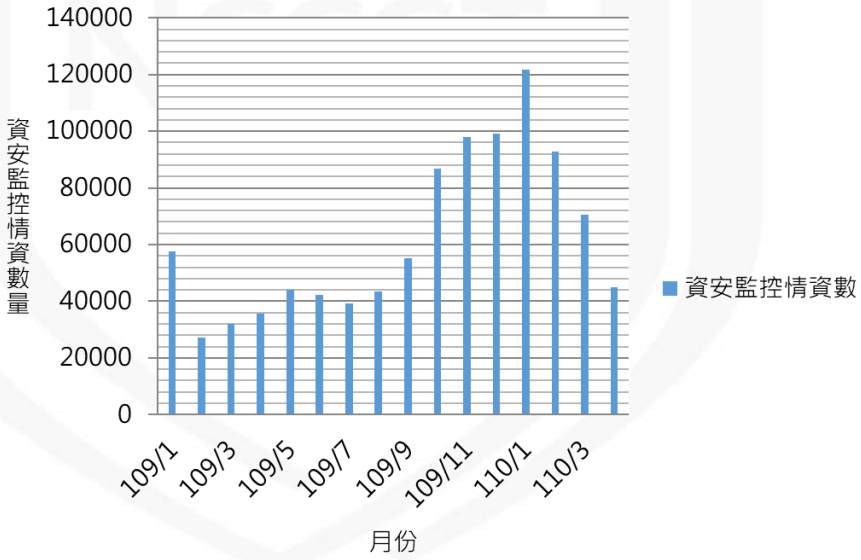
網際網路威脅情蒐分析

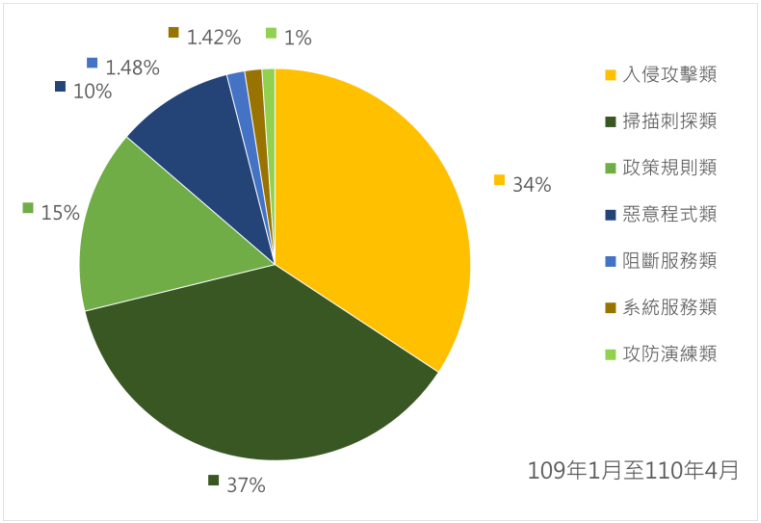
- 109年至110年4月，依技服中心部署之網路威脅誘捕蜜罐(Honeypot)系統，進行網路威脅情資分析
  - 共蒐集1,643個惡意程式，大多透過URL報到、接收指令、下載模組或自主更新，藉此規避防火牆與IDS偵測
  - 共發現530個惡意URL連線
  - 共蒐集128個Android裝置惡意程式，皆屬「Calling Interceptor」殭屍網路



聯防監控情資威脅分析

- 109年至110年4月，SOC業者回傳之聯防監控情資共990,861筆，可明確辨識之前3名威脅
  - 掃描刺探類(37%)：針對已知漏洞、遠端服務及密碼猜測之探測行為
  - 入侵攻擊類(34%)：針對網頁應用程式之攻擊行為
  - 政策規則類(15%)：違反機關資安規範之使用者行為

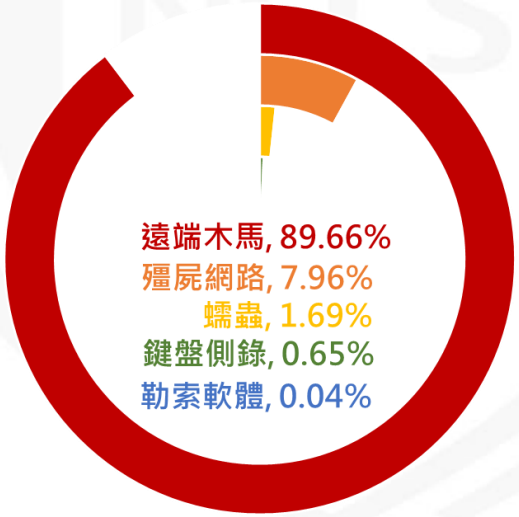


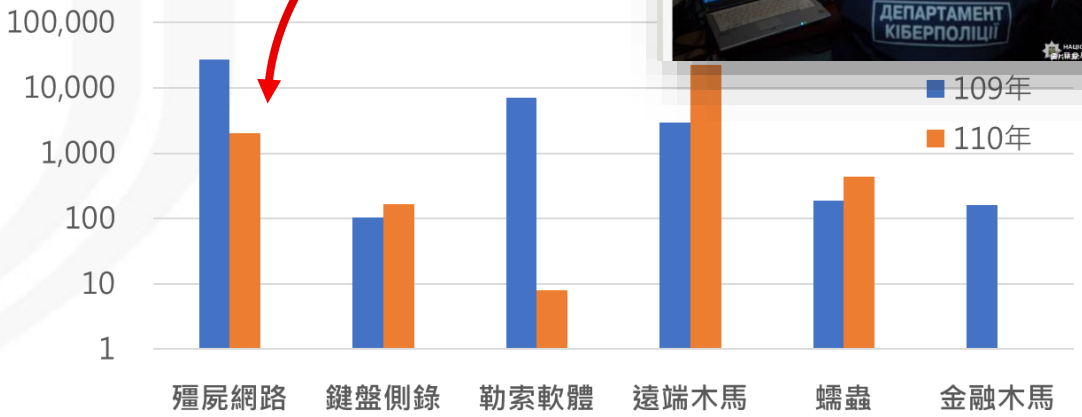


惡意電子郵件趨勢分析(1/2)

- 110年除發現大量駭客利用私密資訊外洩或以重要投資資訊誘導使用者之詐騙與勒索郵件，所偵測之惡意郵件附檔多為遠端木馬惡意程式
- 比對109年數據，可發現惡意電郵附檔之攻擊趨勢從「殭屍網路」、「勒索軟體」轉向散布「遠端木馬」

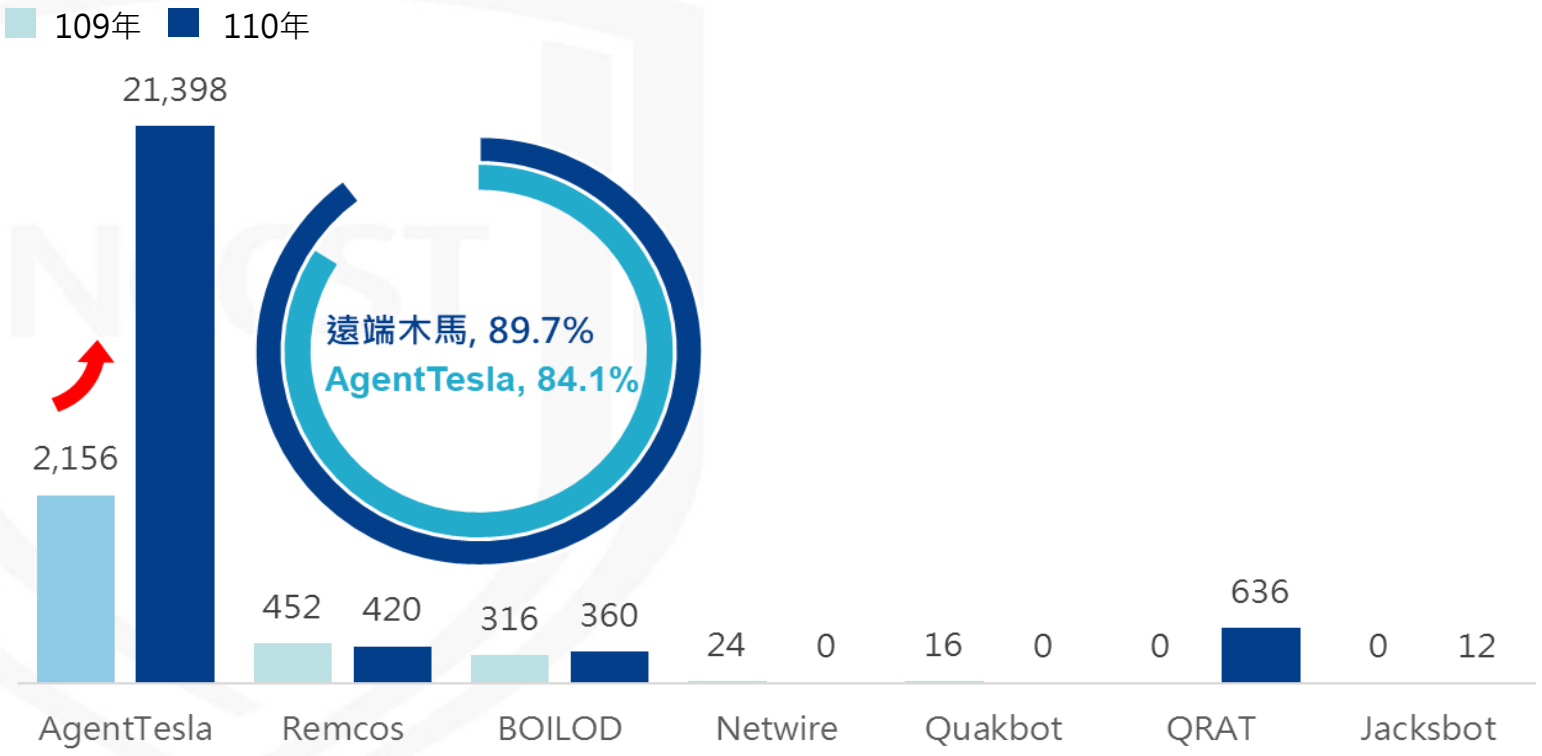
110年觀察到Emotet與其他用來協助散布Emotet之殭屍網路，如：Powload，其數量皆大幅下降





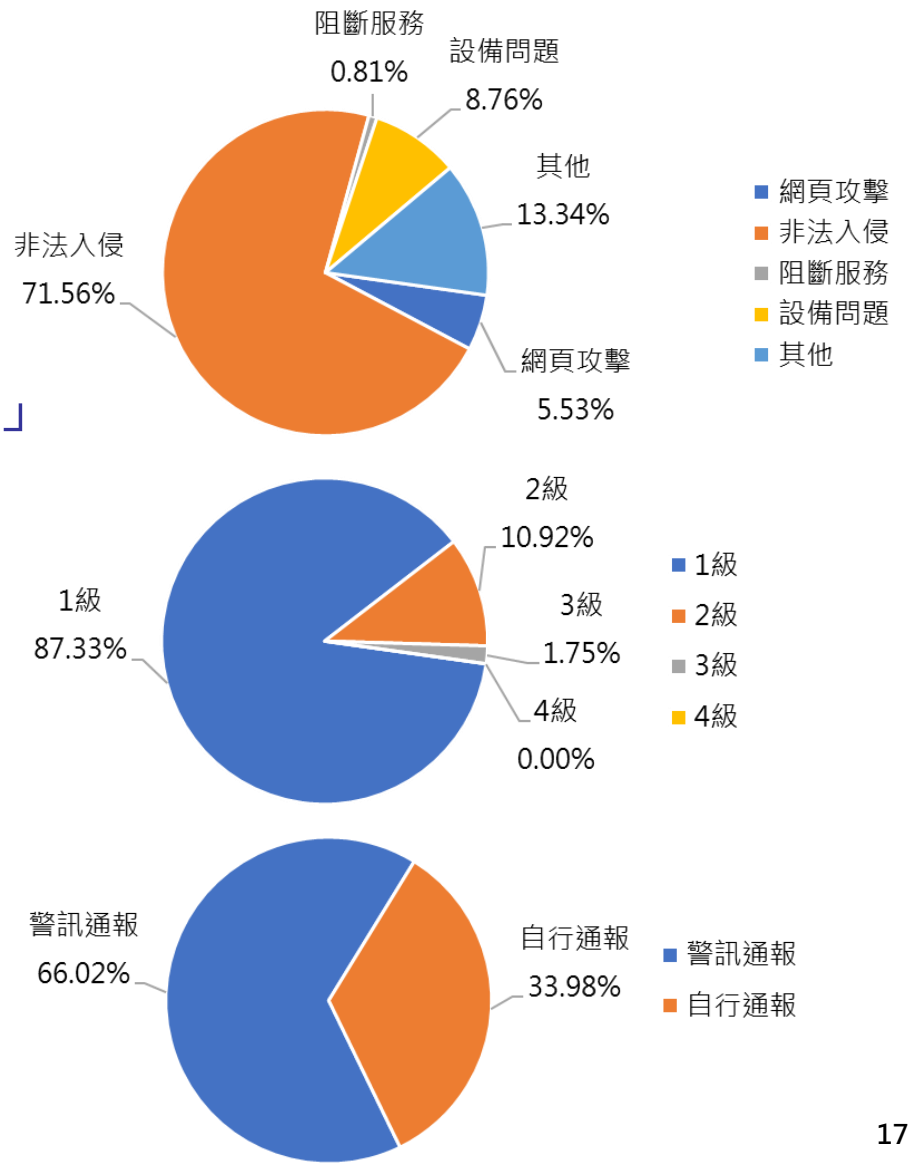
惡意電子郵件趨勢分析(2/2)

- 惡意郵件附檔以「遠端木馬」AgentTesla最為顯著，其數量成長將近10倍之多，惡意文件攻擊則以Office應用程式漏洞CVE-2017-11882與CVE-2017-8570為大宗，此漏洞亦常見於近年APT郵件攻擊



通報事件分析(1/4)

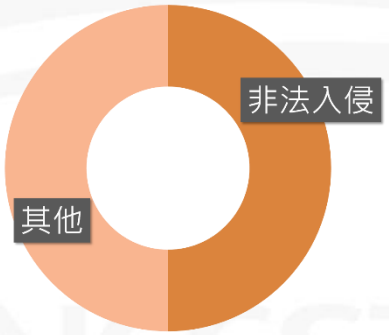
- 分析109年至110年4月通報類型比例，以「非法入侵」類型為大宗，占71.56%，其餘事件可明確分類者，以「設備問題」與「網頁攻擊」為主
- 資安事件影響等級以1級事件為主
- 收到技服中心資安警訊後通報，占所有通報事件66.02%



通報事件分析(2/4)

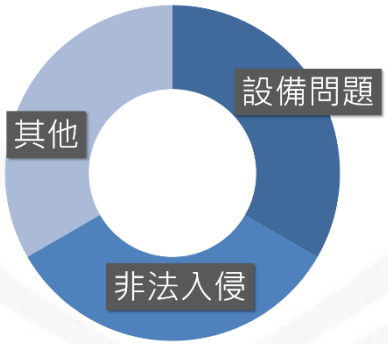
- 109年至110年4月，3級資安事件通報共13件，包含8件資料外洩及5件核心業務中斷

資料外洩發生原因



- 委外廠商人員疏失，誤將未遮蔽之個資放置於活動網站
- 網站遭異常登入，導致含有個人資料之頁面遭非法瀏覽檢視
- 網站設計不當，駭客利用既有上傳功能上傳惡意程式竊取個資

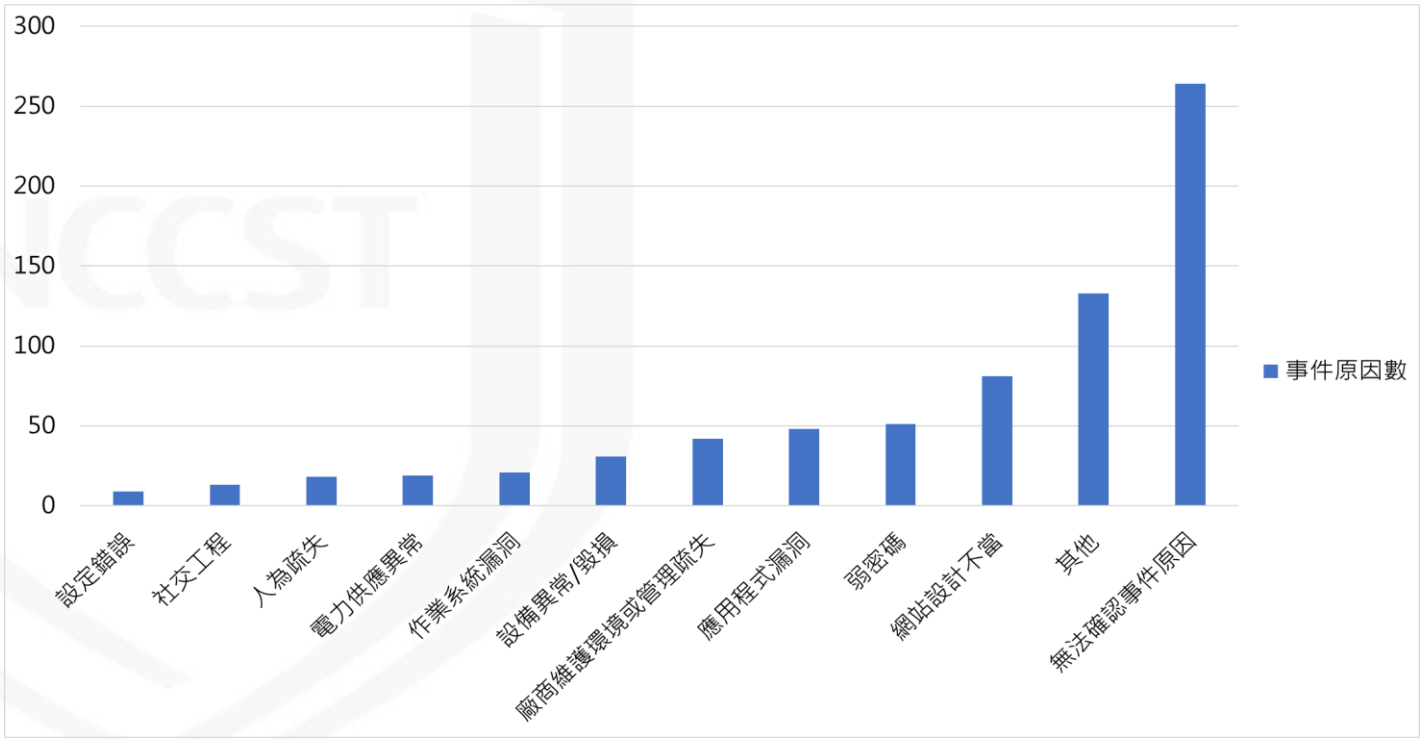
核心業務中斷發生原因



- 系統檔毀損，因無法於可容忍中斷時間內備份還原，影響核心資通系統運作

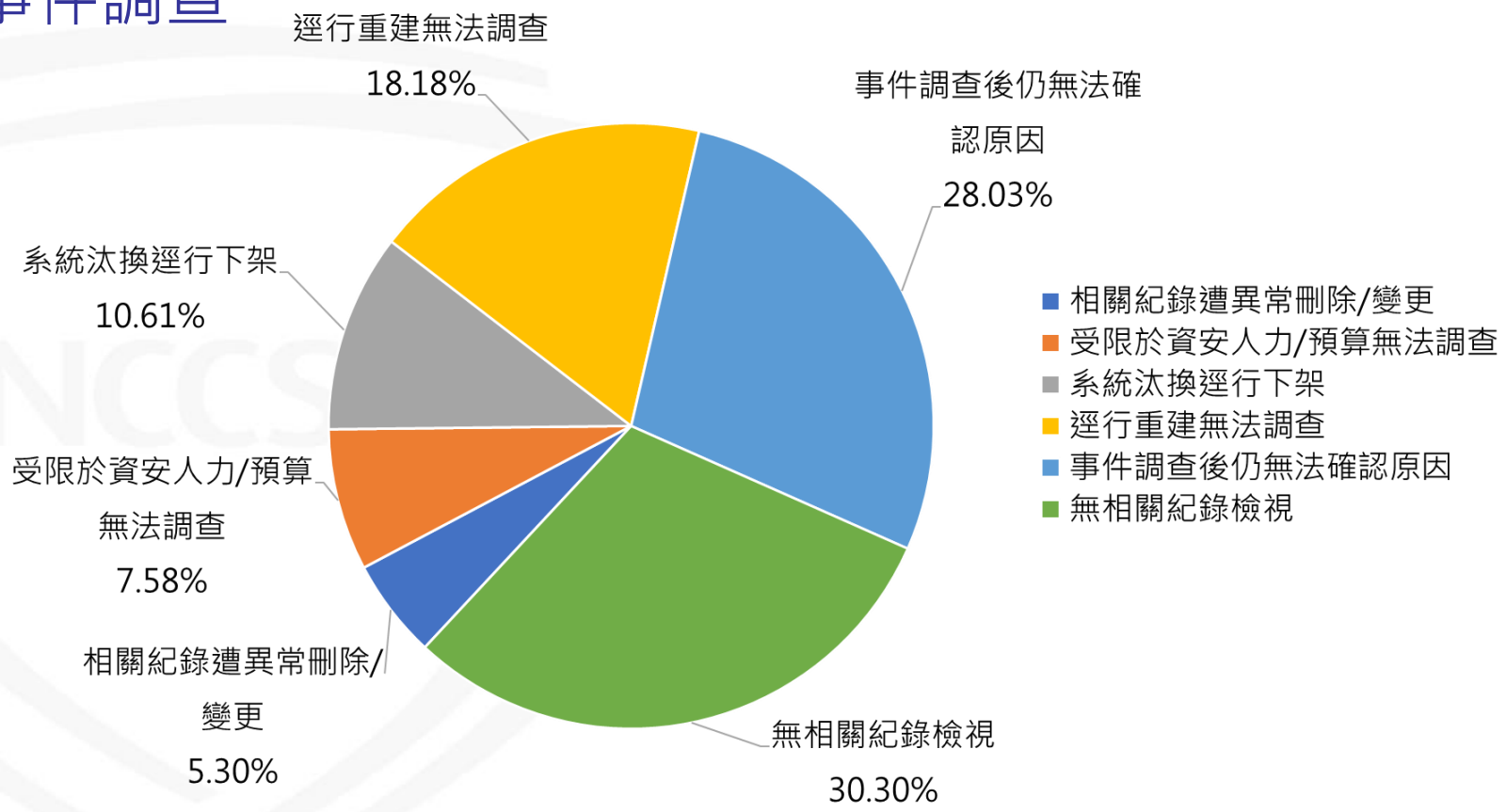
通報事件分析(3/4)

- 綜整109年至110年4月已完成結報之通報案件發生原因，可明確辨識者，以「網站設計不當」、「應用程式漏洞」、「弱密碼」及「廠商維護環境或管理疏失」為主因



通報事件分析(4/4)

- 無法確認事件原因之資安事件，以「無相關紀錄檢視」為主要因素，機關未能保存日誌紀錄，以致無法進行事件調查



政府機關威脅情勢綜合評估

- APT惡意電郵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
- 行動裝置或物聯網設備遭利用擴散惡意程式或殭屍網路，建議使用行動裝置應遵守相關資安規範，同時妥善管理物聯網設備
- 重大資安事件仍以個資外洩造成之衝擊為主，多肇因於網站或權限設計不當，建議機敏資料非必要不得置於公開網站
- 部分資安事件起因「廠商維護環境或管理疏失」，顯示委外廠商資安管理之重要性，應落實委外管理機制
- 資安事件缺乏相關紀錄，以致無法有效針對根因進行改善，顯示對於日誌紀錄保存仍有改善空間

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
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 提升主動防禦能量
  - 符合法規要求強化通報應變機制
- 結論與建議

個人資料外洩案例(個資保護意識)

案情提要

- 某學校新進人員寄信件通知活動人員時，誤將含有機敏資料檔案夾帶於信件中寄出

【機關處置方式】

- 緊急聯繫收件人，請其勿再將資料擴散
- 依個資法規定，通知當事人個人資料外洩情形

防護建議

- 新進人員應加強資安防護意識，避免因人員疏失導致機敏資料外洩
- 若提供個人資料檢視時，宜進行部分資料遮蔽，減緩資料遭揭露後風險

個人資料外洩案例(委外管理)

案情提要

- 某C級機關業務單位委外辦理活動，其委外廠商誤上傳未遮罩敏感資訊之活動資料，致民眾個人資料外洩

【機關處置方式】

- 將誤上傳檔案下架，並於各活動平台公告事件概要，後續規劃建立資料上傳審核機制

防護建議

- 機關應落實委外管理機制，並責成委外廠商應遵守資安管理措施
- 機關可建立資料上傳審核流程，特別是敏感資料之檔案應加強防護

勒索軟體攻擊案例

案情提要

- 某B級機關發現多個設備遭感染勒索軟體，影響日常作業，且核心資通系統無法於可容忍中斷時間內回復正常運作
- 經查為設備維護廠商維運使用之帳號密碼遭外部暴力破解，駭客利用該帳號登入維運設備後，再橫向擴散至其他設備

【機關處置方式】

- 後續以白名單限制系統存取並鎖定來源IP、限制維護廠商帳號及管理者權限帳號專機專用，並重新設置維運使用之帳號密碼

防護建議

- 廠商現場維護可降低資安風險，建議機關設備關閉外部遠端登入
- 管控維護廠商帳號權限，並要求專機專用
- 訂定帳號密碼資安原則，要求維護廠商遵循，並定期檢視其落實度
- 機敏資料除訂定備份頻率外，亦應依資料分級之資安原則限制存取或加密
- 網路應有適當區隔及存取控制，以降低橫向擴散風險

IoT資安弱點攻擊案例

案情提要

- 技服中心偵測發現多個機關資訊設備下載惡意腳本之連線，經機關回報連線設備為監視器設備
- 該監視器設備存在預設帳號密碼漏洞，攻擊者以預設帳密進入設備後，並利用漏洞取得系統完整控制權

【機關處置方式】

- 重置設備、變更監視器預設帳號密碼，並更新韌體版本至最新版本

防護建議

- IoT設備於採購前，應依資通系統防護基準進行評估及測試，確保其安全等級與後續應用範圍
- 應隨時注意原廠所提供之更新資訊，進行測試並完成更新
- 應限制相關設備之網路連線與網域區隔，進行網路連線行為監控與加強存取控制

供應鏈攻擊案例

案情提要

- 某B級機關主機遭植入勒索軟體，經調查發現係廠商維護系統使用之遠端連線管道遭利用，造成機關業務運作停頓

【機關處置方式】

- 中斷主機網路連線，避免橫向擴散
- 透過系統備份重建受駭主機，並加強遠端存取控管

防護建議

- 針對重要服務之資通系統，應建置監控機制，偵測到系統異常時，可即時進行應變處置
- 資通系統維護時，應要求廠商至機關監控環境下進行維護，對於系統遠端維護應採「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，如限制特定存取來源位址、採用雙因子驗證等方式，並監控相關活動
- 要求委外廠商應依資通系統防護基準要求，保存與管理相關日誌紀錄，以利事件鑑識分析

工業控制系統遭植入惡意程式案例

案情提要

- 某D級機關於建置工業控制系統時，因系統測試階段需要，開放外部連線以利廠商調校系統設定
- 偵測發現有惡意程式，經進一步調查發現，該系統於廠商建置環境時已遭入侵，並被植入惡意程式與設定排程

【機關處置方式】

– 中斷主機網路連線，重新架設建置環境

防護建議

- 資通系統應於封閉式環境開發，如需網路服務應規劃嚴謹之存取控制
- 調整工控系統測試環境，關閉不必要通訊埠，限制外部連線來源
- 資通系統正式上線前，除應落實執行弱點掃描、滲透測試等安全性檢測，亦應建置相關資安防護機制

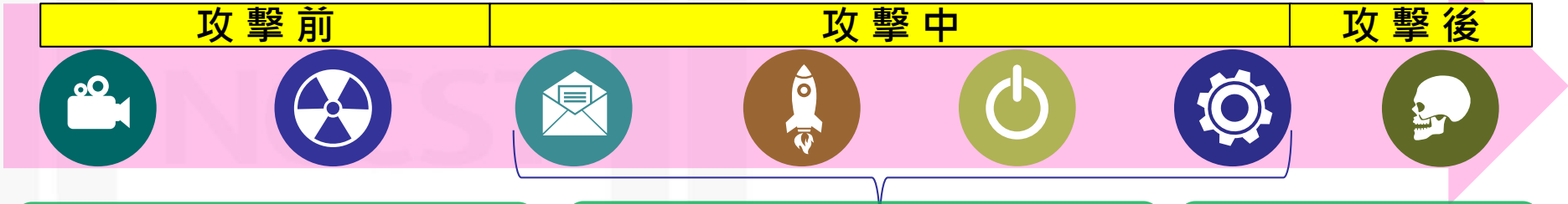
大綱

- 資通安全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
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 提升主動防禦能量
  - 強化通報應變機制
- 結論與建議

提升主動防禦能量

- 駭客狙殺鍊(Cyber Kill Chain)

偵查 (Reconnaissance)	武裝 (Weaponization)	遞送 (Delivery)	攻擊 (Exploitation)	安裝 (Installation)	發令與控制 (Command and Control)	採取行動 (Actions on Objectives)
研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境	針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可遞送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝	設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB媒體等遞送管道	惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊	於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中	受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機	攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性、或是做為入侵其他系統的跳板



加強資安整備	精進縱深防禦	即時應變處置
強化漏洞修補	落實黑名單部署	阻斷APT攻擊
完善備援機制	精進資安監控防護	
落實系統紀錄保存	落實權限控管	
加強資料庫防護		

加強資安整備(1/2)

- 強化漏洞修補
  - 隨時注意重大漏洞訊息，即時修補防護
  - 導入VANS系統，掌握即時訊息
  - 執行滲透測試與紅隊演練，主動發掘資安防護漏洞

- 完善備援機制
  - 做好系統備援，確保服務不中斷
  - 除熱備援與異地備援，宜同時考量資料離線備份，以防勒索軟體攻擊
- 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資料庫等紀錄訊息，以利分析事件根因，改善資安管理

加強資安整備(2/2)

- 加強資料庫防護

機敏資料採取加密、遮罩、混淆等保護機制

定期分析資料庫稽核紀錄，發現潛在異常行為

使用高安全性之加密簽章憑證
使用加密傳輸協定傳遞資料，採行更安全加密演算法

啟用帳號與密碼原則設定，強化帳號密碼安全性

精進縱深防禦(1/2)

- 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
- 精進資安監控防護
  - 妥善規劃資安監控範圍，監控內外異常活動，即時告警
  - 加強關聯分析能量，提升資安監控防護有效性
- 落實權限控管
  - 人員帳號密碼採用最小權限原則，同時配合異常紀錄檢視，監控可疑活動
  - 資通系統權限設定，應納入上線前之檢驗項目
  - 加強供應商管理與來源管制，遠端連線原則禁止例外開放

精進縱深防禦(2/2)

- 針對供應商連線至機關內部環境應加強來源管制，遠端連線原則禁止例外開放

1. 存取期間原則以**短天期**為限
2. 建立**異常**行為**管理**機制
3. 結束後，**確實關閉**網路連線
4. **更換**遠端存取通道(如VPN等)登入**密碼**

※雲端服務之使用不在此禁止範圍

行政院資安處110年3月2日院臺護字第1100165761號函

即時應變處置

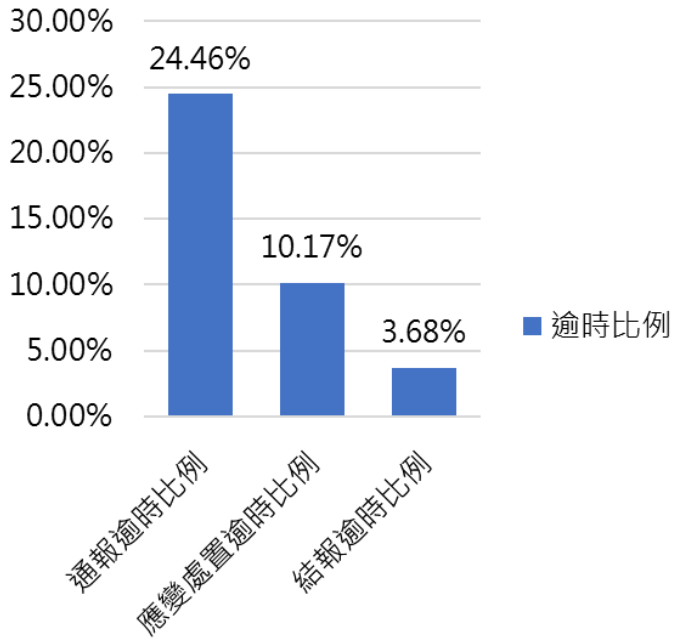
- 阻斷APT攻擊
  - 機關資安防護設備如IPS/IDS等，部署APT攻擊偵測規則，即時阻斷駭客攻擊
  - 近期發現APT攻擊常使用正常雲端空間服務做為中繼站，若機關未禁止同仁使用公開雲端服務，應建立相關防護規範，並加強控管

大綱

- 資通安全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
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 提升主動防禦能量
  - 強化通報應變機制
- 結論與建議

強化通報應變機制(1/4)

- 遵循「資通安全事件通報及應變辦法」，於規定時間內完成事件通報、復原及緊急應變處理，以在最短時間內恢復系統運作
  - 分析109年至110年4月資安事件逾時情形，通報逾時24.46%、應變處置逾時10.17%及結報逾時3.68%
- 歸納常見逾時因素
  - 未定期更新通報應變網站登入資料，以致無法登入操作
  - 未明確定義內部通報應變機制，以致機關內部跨部門不熟悉通報流程



強化通報應變機制(2/4)

- 「事件通報及應變處理作業程序」要求事項落實各機關資通安全

事項	說明
通報 資通安全事件	• 第3級或第4級資通安全事件，應以電話方式通知上級機關或中央目的事業主管機關，若無上級機關者，應通知主管機關
辦理 事件應變會議	• 完成第3級或第4級資通安全事件之初步損害控制後，辦理事件應變會議
損害控制 或復原作業	• 第3級或第4級資通安全事件，定時向上回報控制措施成效 • 若涉及個資外洩，應評估通知當事人之適當方式，依個資法第十二條規定辦理
事件根因分析	• 如發現惡意程式，應上傳至Virus Check網站進行檢測，送交防毒軟體或資安服務公司檢測 • 進行根因調查，並提出紀錄分析
改善追蹤	• 第3級或第4級資通安全事件，應另以密件公文送交調查、處理及改善報告至送交主管機關及上級或監督機關

強化通報應變機制(3/4)

- 各機關於日常維運資通系統時，依資通安全責任等級保存日誌紀錄，並定期備份於外部設備
- 應落實執行必要之跡證保存，以利進行事件根因分析

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。	1. 作業系統日誌(OS event log) 2. 網站日誌(web log) 3. 應用程式日誌(AP log) 4. 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。	

強化通報應變機制(4/4)

- 配合技服中心警訊通知進行應變處置

警訊類型	警訊說明	機關應變處置
資安預警警訊(EWA)	技服中心偵測機關疑似異常連線、對外攻擊或是下載惡意程式，即發布資安預警警訊	建議機關針對警訊內容進行檢視，若發現有入侵事實，則須依循資通安全管理法，執行資安通報作業
入侵事件警訊(INT)、網頁攻擊警訊(DEF)	技服中心偵測確認機關遭受資安事件影響	機關應於收到警訊通告後，循機關內部程序上報外，並須依循資通安全管理法，執行資安通報作業
漏洞/資安訊息警訊(ANA)	技服中心寄發資安訊息警通知機關重大漏洞/資安訊息	機關若經相關檢測後，發現遭入侵情事，仍需至通報應變網站進行通報登錄
緊急應處警訊(ALT)	技服中心針對影響範圍廣泛資安風險，發布警訊通知機關調查受影響情形	應先至通報應變網站檢視事件調查表內容，確認事件調查項目，掌握調查重點與內容

緊急應處警訊說明(1/2)

- 緊急應處警訊係針對影響範圍廣泛資安風險，發布警訊通知機關調查受影響情形
  - 重大漏洞與其修補情形
    - 針對重大漏洞調查機關是否在漏洞影響範圍，並掌握機關是否完成漏洞修補
  - 資通系統使用情形
    - 若接獲特定資通系統具安全性問題，將調查機關是否使用該系統，並確認是否具該安全性問題
  - 其他經評估有調查必要事項
    - 除前述調查事項，其他如資料外洩確認或機關存在異常連線確認等需調查確認，亦會發布緊急應處警訊通知相關機關

緊急應處警訊說明(2/2)

- 機關在接獲ALT警訊時，應先至通報應變網站檢視事件調查表內容，確認事件調查項目，掌握調查重點與內容
- 調查過程中，如發現資訊設備已遭駭客利用漏洞入侵，仍應依「資通安全事件通報及應變辦法」，進行資安事件通報
  - 例如：110年3月技服中心針對Microsoft Exchange Server漏洞進行調查，機關接獲緊急應處警訊至通報應變網站回覆調查狀況

行政院國家資通安全會報技術服務中心

緊急應處警訊

發布編號	NCCST-ALT-2021-0000001	發布時間	Tue Mar 09 11:3 31 CST 2021
事件類型	系統弱點	發現時間	Tue Mar 09 00:00: 00 CST 2021
事件主旨	微軟 Microsoft Exchange Server 漏洞影響調查		
事件描述	微軟 2021 年 3 月 2 日針對 Microsoft Exchange Server 發布 4 個重大安全性漏洞(警訊編號：NCCST-ANA-2021-0000042)修補公告，受影響版本包含 Microsoft Exchange Server 2013、Microsoft Exchange Server 2016 及 Microsoft Exchange Server 2019。由於已有駭客利用上述漏洞發起攻擊活動，為掌握各機關影響情形，請各機關儘速調查郵件伺服器使用與更新 1 年 3 月 12 日前至通報應變網站回覆調查結果，調查範圍 關使用郵件伺服器 二、機關所屬公務機關郵件伺服器		
因應對策	參考 NCCST-ANA-2021-0000042 警訊進行修補更新		
參考資料	https://us-cert.cisa.gov/ncas/current-activity/2021/03/06/microsoft-exchange-server-vulnerabilities https://techcommunity.microsoft.com/t5/exchange-team-blog/mar-server-security-updates-for-older-cumulative/ba-p/2192020		

警訊事件調查列表

項次	發布編號 / 警訊名稱	寄件時間	填報時間	處理完成時間	功能
1	NCCST-ALT-2021-0000001 / 請回報ALT報表	2021-04-28 14:23:51	尚未填報	尚未處理完成	填報

大綱

- 資通安全威脅趨勢與案例分享
  - 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享
- 政府機關資安防護強化重點
  - 提升主動防禦能量
  - 強化通報應變機制
- 結論與建議

結論與建議(1/3)

- 依據機關通報之資安事件，歸納以下建議
  - 監視器等物聯網設備易疏於管理與維護，建議定期檢視與落實安全性更新，並透過防火牆進行存取控制
  - 資通系統維護時，應要求委外廠商至機關監控環境下進行維護，對於遠端維護應採「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，如限制特定存取來源位址、採用雙因子驗證等方式，並監控相關活動，降低供應鏈遭攻陷成為資安防護破口風險
  - 機關通報之資安事件，仍以技服中心警訊通知為主，機關可強化主動防禦能量，及早自行發現與防範

結論與建議(2/3)

- 因應資安威脅趨勢，機關可提升主動防禦能量，並落實資安防護策略
  - 攻擊前加強資安整備：強化漏洞修補、完善備援機制、落實系統紀錄保存及加強資料庫防護
  - 攻擊中精進縱深防禦：落實黑名單部署、精進資安監控防護及落實權限控管
  - 攻擊後即時應變處置：阻斷APT攻擊

結論與建議(3/3)

- 機關應遵循與落實法規要求，強化通報應變機制
  - 依照「資通安全事件通報及應變辦法」，於規定時間內完成事件通報、復原及緊急應變處理
  - 落實「各機關資通安全事件通報及應變處理作業程序」要求事項，並完善跡證保存
  - 接獲技服中心警訊通知，應配合辦理通報與應變處置
  - 若接獲緊急應處警訊，需依照警訊說明於時限內完成調查，並回覆至通報應變網站

報告完畢
敬請指教