110 年國家資通安全情勢報告

行政院

中華民國 111 年 6 月

目次

圖目次

壹、依據及目的

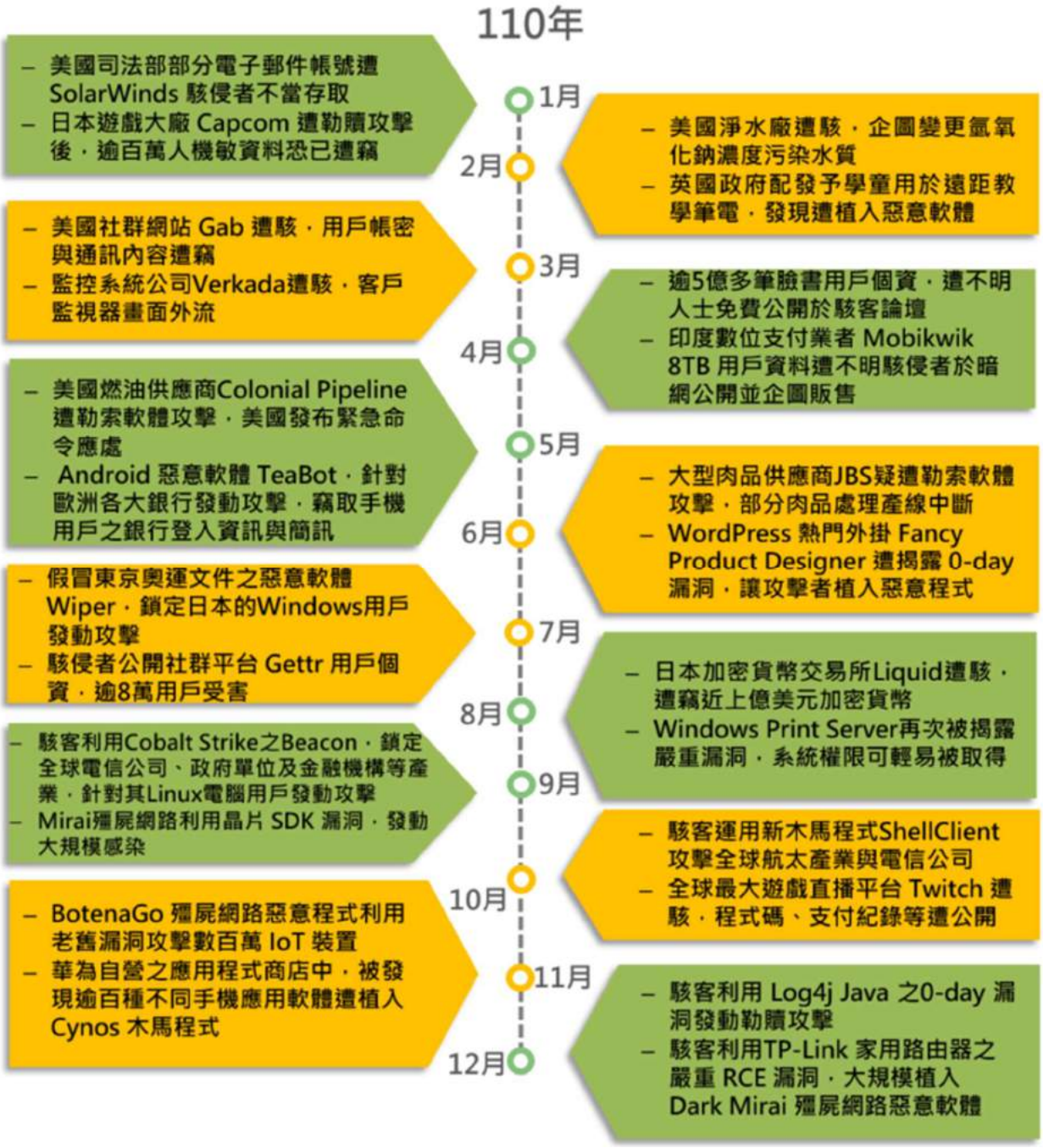
資通安全管理法(以下簡稱資安法)業於 108 年 1 月 1 日正式施行,本院依據資安法第 5 條規定,定期公布「國家資通安全情勢報告」。

隨著資通訊科技進展與應用普及,個人、社會及國家所面臨之資安挑戰愈來愈大,駭侵威脅程度甚至已提升至國安層級,有鑑於資安即國安,本院已於 110 年 2 月公布第六期國家資通安全發展方案(110 年至 113 年,以下簡稱第六期發展方案),研議資安整體發展策略,並提出強化主動式防禦相關技術研發與應用為深化我國資安政策或供研擬其配套措施參考;本報告藉由研析 110 年全球資通安全威脅情勢及我國政府機關所面臨之資通安全威脅現況,提出相關資安防護建議,協助各機關強化資通安全防護能量,期經由前瞻政策引導及國家整體資源力量,打造安全可信賴之數位國家。

貳、110 年全球資安威脅情勢概要

根據世界經濟論壇(World Economic Forum, WEF)發布之 110 年全球風險報告統計，經濟、環境、地緣政治、社會及科技等 5 大類風險中，科技類型風險以「網路安全失效(Failure of Cybersecurity Measures)」為最高，並包含惡意技術利用、技術治理失效、數位權利集中及 IT 基礎架構失效等項。當缺少資安防護時，將可能為網路犯罪所攻擊，造成經濟損失，甚至影響政治與社會安定，該報告進一步指出，相關惡意技術工具被不當使用，將帶來更激進之攻擊方法，再加上缺乏資安專業人員及完善之治理機制，資安威脅日益加劇。

隨著新冠肺炎(COVID-19)的疫情發展，全球持續採取遠距辦公、居家學習，因疫情而漸趨普遍之居家辦公(Work From Home, WFH)工作模式，帶來資訊設備、身分驗證及居家實體環境等使用情境上不同之挑戰，由於對資通訊服務之依賴仍持續擴大，駭客轉移攻擊目標，導向不斷擴展的網路邊緣和環境，讓資安威脅越演越烈，如同疫情無法藉由邊界封鎖完全控制，網路攻擊事件、跨境攻擊亦無可倖免。觀測 110 年全球重大網路攻擊事件，個人憑證或帳密之外洩事件屢見不鮮，且因社群媒體發達與民眾資安防護意識尚未完善，皆導致個資外洩事件之影響無法緩解。此外，隨著物聯網(Internet of Things, IoT)設備普及，系統漏洞未即時修補與更新，增加設備安全性衝擊外，駭客亦透由勒索軟體、進階持續性威脅(Advanced Persistent Threat, APT)攻擊等手法，致使各國企業、政府機關受到波及，尤以民生相關之水資源、油電等關鍵基礎設施者相關攻擊所造成的影響，實不容輕忽，特整理 110 年全球重大網路攻擊事件(詳見圖 1)供參。



資料來源：本院國資通安全會報技術服務中心整理

圖 1　110 年全球重大網路攻擊事件簿

經綜整分析歐盟網路暨資訊安全局(European Union Agency for Cybersecurity, ENISA)、澳洲網路安全中心（Australian Cyber Security Centre，ACSC）及各資安業者調查等報告資料，歸納出各國 110 年資安威脅情勢，包含「疫情造成資安風險提高」、「勒索軟體攻擊風險

激增」、「物聯網與行動式設備資安弱點威脅升高」、「資安(訊)供應商遭駭破壞供應鏈安全」、「進階持續威脅鎖定式攻擊竊取機密資料」及「社交工程詐騙盛行」等 6 項。

一、疫情造成資安風險提高

因應新冠肺炎疫情影響，居家辦公轉變為常態，視訊會議、行動式設備及雲端需求與應用大幅提升，遠端存取、應用、基礎設施及服務之資安議題亦隨之浮現，擴展資安邊界將產生管理多面向之挑戰。

美國國土安全部網路安全暨基礎安全局（Cybersecurity and Infrastructure Security Agency, CISA）於 110 年發布警訊指出，常被攻擊者利用之 12 個漏洞中，超過半數為遠端工作環境所需之 VPN 連線或雲端服務相關漏洞，顯示駭客利用遠距工作之龐大需求，積極尋找相關資通訊技術弱點，多方面挖掘居家辦公之資安破口。此外，亦有配合疫情緊急開發之系統，因系統發展上線程序未如一般系統嚴謹，致存有資安破口，易受駭侵利用。研究機構 VPNMentor 曾指出，印尼政府所開發之防疫追蹤 APP(eHealth Alert Card)有遭入侵案例，肇因為該 APP 之資料庫配置錯誤，且未妥善防護，導致約 130 萬人之 COVID-19 檢測資訊、醫療紀錄及個資等機敏資訊外洩，有心人士可透過公共伺服器取得曾透過該程式登錄之國內外旅客的個人資料，內容包含姓名、身分證號碼、COVID-19 病毒篩檢結果、住處及其他個人醫療等相關資訊。

二、 勒索軟體攻擊風險激增

世界經濟論壇發布之 110 年全球風險報告指出，惡意軟體與勒索軟件攻擊分別增加 358%與 435%，其攻擊次數為倍數以上之成長，隨著勒索軟體即服務(Ransomware-as-a-Service, RaaS)興起與網路犯罪生態體系形成，推波助瀾讓勒索軟體之威脅範圍與經濟損失

日漸擴增。另據資安業者 Sophos 對逾 5,400 個組織調查報告(The State of Ransomware 2021)，110 年被勒索軟體攻擊所造成之平均成本(含贖金、人事成本、設備成本及營運損失等)已達 185 萬美元，較 109 年之受害金額 76 萬美元更為嚴重。

知名勒索軟體受駭案例為美國最大燃油供應業者 Colonial Pipeline 於 110 年 5 月 7 日遭勒索軟體攻擊，暫停所有輸油管線運作，美國能源部於兩日後迅速宣布進入緊急狀態(State of Emergency) ，特例允許當地燃油業者透過一般道路運送燃油，以緩解燃油短缺問題，同時該業者得知遭勒索軟體攻擊後，立即將特定系統離線以控制威脅，包含暫時關閉所有輸油管線作業與部分資訊系統，同時聘請第三方資安專家調查此一事件性質與影響範圍，並與執法機關保持聯繫。

三、物聯網與行動式設備資安弱點威脅升高

資安業者 Check Point 110 年網路安全報告調查數據顯示，計有 46%企業至少有 1 名員工曾於手機下載惡意軟體，且隨著手機使用量增加，銀行木馬與手機木馬程式數量亦不斷增長；另該公司於 111 年網路安全報告中亦指出，曾發現惡意攻擊者持續一整年對行動式設備使用者與特定企業展開攻擊，惟因許多工作場所實施自攜裝置（Bring Your Own Device, BYOD）政策，約有 49%受訪對象表明其組織無法檢測到員工自帶設備所遭受之攻擊或事件。

隨著物聯網裝置普及且運用廣泛，惟若疏於管理可能造成莫大影響，資安事件案例常發現殭屍網路惡意程式利用老舊漏洞，攻擊物聯網裝置。大型電信業者 AT&T 之資安實驗室 Alien Labs 於 110 年 11 月揭露，新型殭屍網路惡意程式 BotenaGo 利用 33 個已知之老舊資安漏洞，鎖定包含網路路由器、數據機、網路儲存裝置等數百萬台物聯網設備發起攻擊行動，而該惡意程式成功入侵設備後會

執行遠端 Shell 指令，並依受感染設備類型，下載不同惡意封包資料(Payload)，惟駭客現已刪除伺服器上所有惡意封包資料，使資安研究人員仍無法得知駭客最終企圖。

四、資安(訊)供應商遭駭破壞供應鏈安全

歐盟 ENISA 於 110 年發布之供應鏈威脅報告(Threat Landscape for Supply Chain Attacks)中指出，供應鏈攻擊仍持續增長，且影響範圍也更為廣大，該報告並指出約 66%事件攻擊者係針對供應商程式原始碼，58%攻擊目標是客戶端資料，如個人資料與智慧財產等，隨著對供應鏈之依存性越來越高，供應鏈資安威脅亦與日俱增。

110 年資安業者 ESET 揭露一起自 109 年 9 月起針對手機遊戲模擬器 NoxPlayer 之供應鏈攻擊行動，該手機模擬器於全球擁有 1.5 億使用者，而這起攻擊所針對範圍以我國、香港及斯里蘭卡為主，其攻擊手法主要為利用軟體更新機制，首先控制 NoxPlayer 之伺服器，於用戶執行更新時，即以受控制之伺服器將惡意程式植入用戶端，該惡意程式主要蒐集用戶資訊，包含用戶鍵盤輸入紀錄與機敏資訊等。此外，亦有資安業者 Sonatype 指出，程式語言 Python 官方認證之第三方程式庫(Python Package Index, PyPI)，存在多個含有挖礦程式碼之惡意套件，利用與知名常用軟體近似命名，混淆軟體開發者，藉此增加下載量，該惡意套件一經軟體開發者執行，會另行下載惡意程式，並利用開發者電腦中之運算資源進行加密貨幣挖掘。對於此類攻擊，受駭侵者除軟體開發者本身的系統外，亦包含相關透過惡意程式碼開發之產品，在軟體供應鏈安全性方面有相當風險。

五、進階持續性威脅攻擊竊取機密資料

資安業者 FireEye 於 110 年資安洞察報告(Cyber Security Insights)指出，最容易被 APT 鎖定式攻擊之前 5 個行業分別是商業

與專業服務、零售與餐飲、金融、醫療保健及高科技產業，且在過去 10 年中，商業與專業服務、金融一直是位居前 5 名最易被鎖定之行業別；此外，除前述行業別外，關鍵基礎設施也同為駭客入侵目標，如資安業者 Dragos 於 2020 工業控制系統安全年度報告即列舉 4 個鎖定關鍵基礎設施之新駭客組織，分別為 Stibnite、Talonite、Kamacite 及 Vanadinite，其 APT 鎖定式攻擊領域包含電力、能源、製造及運輸等，可見駭客集團已形成特定目標之攻擊模式，運用進階持續性威脅攻擊手法竊取資料或破壞其業務之正常運作。

110 年美國關鍵基礎設施遭 APT 鎖定式攻擊之受駭案例為美國佛羅里達州淨水處理廠遭不明駭客入侵，試圖調高水中氫氧化鈉(Sodium Hydroxide)濃度；佛羅里達州警方說明，該州轄下奧德馬爾(Oldsmar)市淨水處理廠員工於 110 年 2 月 5 日發現，內部電腦遭不明駭客透過桌面共享軟體 TeamViewer 連線存取，試圖將水中氫氧化鈉濃度從正常之 100 ppm 調高至 11,100 ppm，由於氫氧化鈉為高腐蝕性強鹼，於淨水過程中添加可中和酸鹼質與去除金屬離子，若人體攝入過高濃度氫氧化鈉，會造成呼吸道腫脹、痙攣及肺部發炎等症狀。根據調查，可能發生原因包含使用微軟已停止支援之作業系統 Windows 7、允許遠端使用桌面共享軟體、未安裝防火牆防護及共用密碼，且未限制相關電腦及系統監控與資料擷取功能(Supervisory Control And Data Acquisition, SCADA)系統間之連結等不安全使用行為所造成。

六、社交工程詐騙盛行

資安業者 Fortinet 於 110 年營運技術和網路安全報告(2021 State of Operational Technology and Cybersecurity Report)指出，相關業者常面臨之入侵手法包含網路釣魚與惡意軟體，其中因網路釣魚而引起的資安事件較 109 年增加 43%；資料外洩事件有 42%來自於企業

內部，較 109 年增加 18%；另資安業者趨勢科技於 110 年網路安全報告亦指出，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及各種管制訊息，再將使用者導向與疫情相關之詐騙或假訊息網站。

資訊廠商微軟於 110 年 5 月表示，主導 SolarWinds 供應鏈攻擊行動之國際駭客組織 Nobelium，鎖定政府機關、研究機構、非政府組織及國際組織，發起新一波攻擊行動。駭客組織藉由獲取美國國際開發總署(United States Agency for International Development, USAID)所使用之 Constant Contact 帳號，寄送惡意釣魚郵件予全球 24 個國家，逾 150 個組織之 3,000 個電子郵件帳號，其郵件內容嵌入惡意連結；受駭者先被引導至合法 Constant Contact 服務網頁，再跳至駭客掌握之網頁，接續將惡意程式植入受駭者之系統，使駭客可常駐於受駭系統，以利後續進行橫向移動或竊取資訊等惡意行為。微軟進一步指出，依據該駭客組織過往行動模式，其一貫之攻擊策略為入侵供應商，進而攻擊供應商之客戶。

參、110 年政府資安威脅統計

一、聯防預警情資

為協助公務機關資通安全威脅情勢，行政院國家資通安全會報技術服務中心定期綜整資安監控情資，以掌握資安威脅類別及趨勢，並提供政府資安監測預警與服務。

經統計 110 年期間所彙整之監控情資，並將資安威脅類別區分為入侵攻擊類、掃描刺探類、政策規則類、惡意程式類、阻斷服務類、系統服務類及攻防演練類等 7 類，第 1 名為入侵攻擊類(41.0%)，主要針對系統攻擊以獲取非法權限，包含網頁入侵行為、國外 IP 攻擊行為等；第 2 名為掃描刺探類(26.0%)，係針對已知漏洞、遠端服務及密碼猜測之探測行為，包含弱點掃描、外部主機執行掃描探測攻擊等；而第 3 名為政策規則類(17.0%)，主要為針對違反機關資安規範之使用者行為，包含特權帳號於非上班時間登入、帳號由預期外之主機登入等行為，各類資安威脅分布詳圖 2。

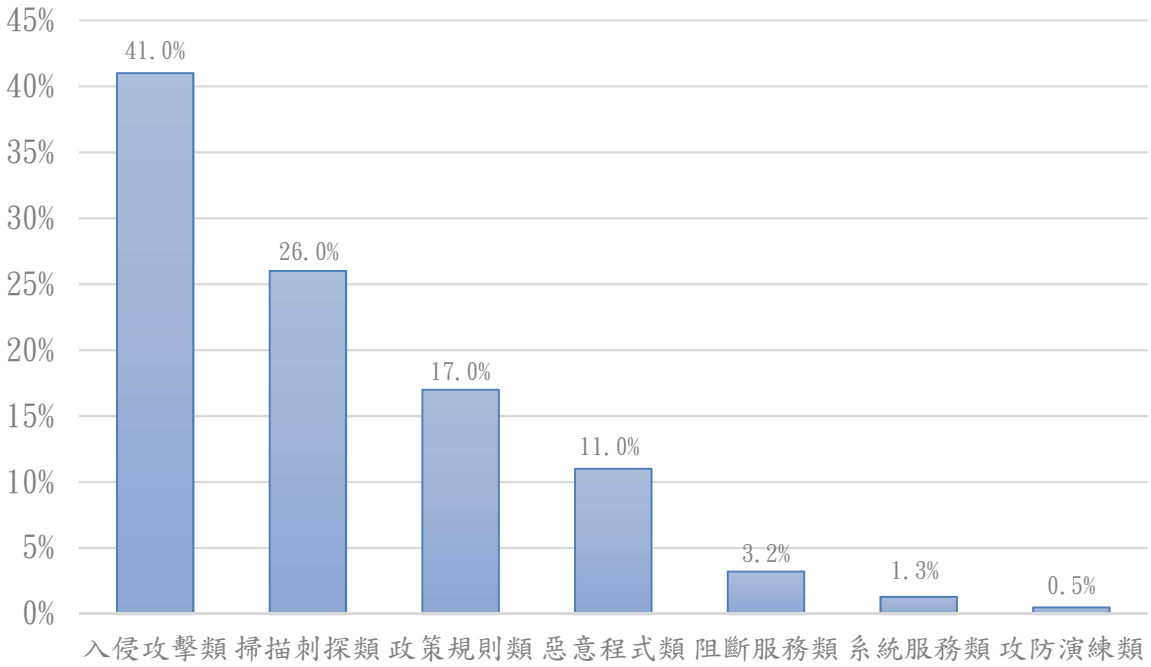


圖 2　各類資安威脅分布圖

二、惡意電子郵件分析

惡意電子郵件為政府機關主要資安威脅來源之一，因現今防火牆與網路相關防護設備趨於普及，駭客較難經由網路服務入侵一般使用者終端電腦。因此，駭客藉由寄送夾帶惡意文件檔案之電子郵件至目標信箱，如社交工程、釣魚郵件及垃圾郵件等，透過公務或時事相關主旨誘騙目標使用者開啟惡意檔案或可疑連結，使目標電腦遭受被惡意程式(諸如殭屍網路、勒索軟體及遠端木馬等)感染控制之威脅，進而導致機敏公務資料外洩風險提高。

從 110 年政府機關惡意電子郵件偵測資料(如圖 3)中，3 月、4 月、8 月、11 月及 12 月偵測到大量詐欺釣魚郵件散布，經進一步分析發現 4 月釣魚郵件係駭客偽冒政府機關郵件帳號，以重要交易名義為由，要求收件人回覆個人資訊之惡意郵件；其餘 3 月、8 月、11 月、12 月等月份，則是假藉取得收件人電腦機敏資訊或掌握使用者不堪影片為由，企圖向收件人勒索比特幣。

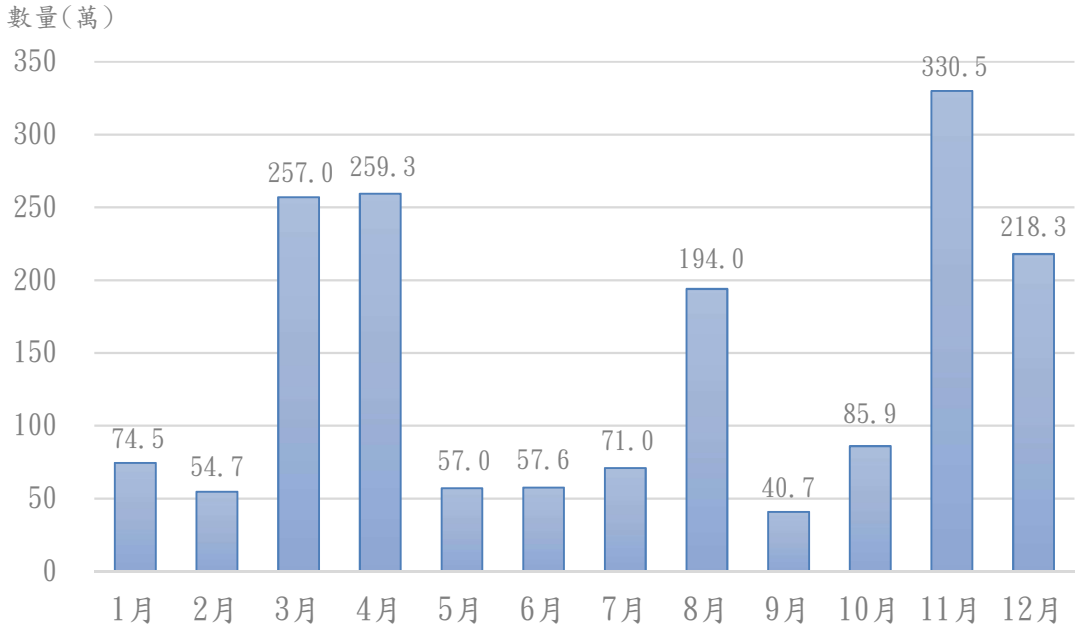


圖 3　110 年各月惡意電子郵件偵測數量統計

三、資安攻防演練

為檢測政府機關資安防護能力，並強化遭遇資安事件時之緊急應變、系統復原及協調管控等作業反應，爰透過官學研界合作，邀集國內資安專業人員，運用駭客常用手法，對政府機關資通系統進行攻擊，檢測政府機關及所轄對外系統之資安防護能力，並據以研討機關資安防護精進作為；110 年計 65 個機關參與演練，演練內容包括「資通系統實兵演練」及「社交工程演練」兩類，110 年演練結果說明如下：

(一)資通系統實兵演練結果

針對機關存在之資通系統弱點進行攻擊，就機關受攻擊後產生之衝擊性分為重大衝擊性、高衝擊性、低衝擊性及尚無衝擊性 4 種類型，演練結果計有 30 個機關發現低衝擊性以上之弱點，占演練機關總數 46.15%。

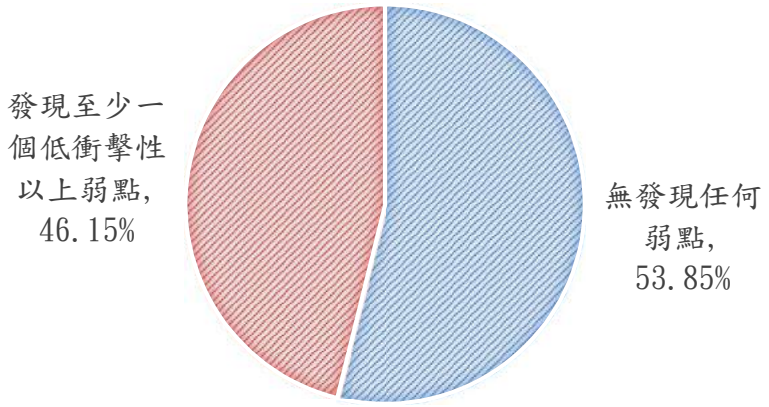


圖 4　發現弱點機關比例

本次演練共發現 95 個弱點，其中重大衝擊性弱點數量 1 個，占整體弱點數量 1.05%，高衝擊性弱點數量 40 個，占整體弱點數量 42.11%；中衝擊性弱點數量 6 個，占整體弱點數量 6.32%；低衝擊性弱點數量 48 個，占整體弱點數量 50.52%(詳見圖 5)。

另依 110 年網路攻防演練所發現之弱點涵蓋 6 種類型，依弱點數量排序分別為無效的身分認證(50%)、無效的存取控管(20%)、不安全的組態設定(19%)、跨網站腳本攻擊(8%)、注入攻擊(2%)及使用已知漏洞元件(1%)；其中「無效的身分認證」、「無效的存取控管」及「不安全的組態設定」等 3 類占總弱點數量約 9 成，主要是機關未落實基本安全設定，常見問題包含允許使用者設定與帳號相同之通行碼、系統使用者可繞過身分驗證機制及未強制要求使用者修改預設通行碼等項，顯示演練機關之資通系統仍存在一定程度之風險與威脅。

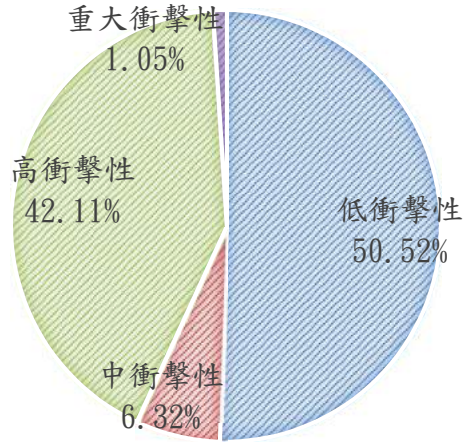


圖 5　弱點衝擊比例分布圖

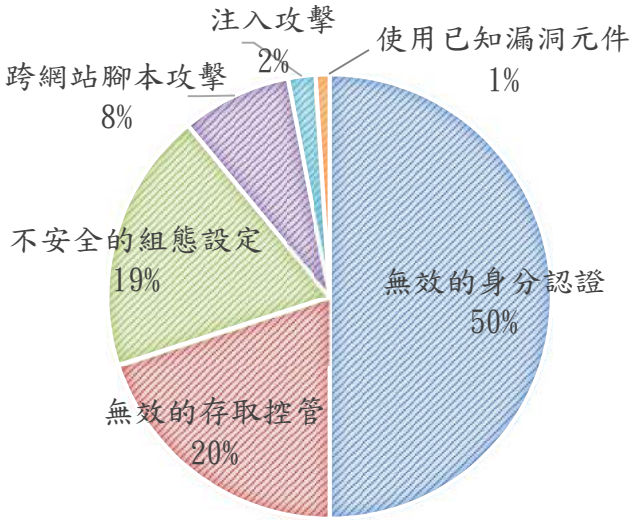


圖 6　弱點類型數量分布圖

(二)社交工程演練結果

隨機寄發社交工程郵件與簡訊，並記錄使用者「開啟郵件」、「點閱郵件附件或連結」及「點閱簡訊連結」等行為。

本次郵件演練結果，開啟郵件計有 46 個機關，占演練機關數量之 70.8%，參演機關人員開啟郵件比率為 4.1%；點閱連結或附件者有 41 個機關，占演練機關數量 63.1%。

另，簡訊演練計有 63 個機關，點閱簡訊連結者有 37 個機關，占演練機關數量 58.7%；參演機關人員點閱簡訊連結有 261 個門號，占演練門號 16.9%。

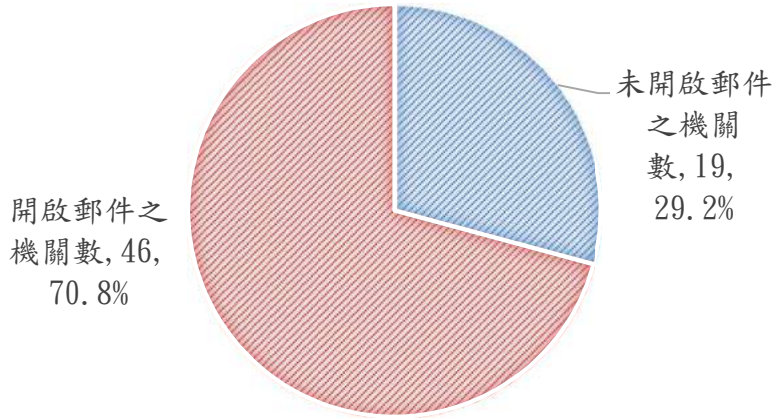


圖 7　開啟郵件機關比例圖

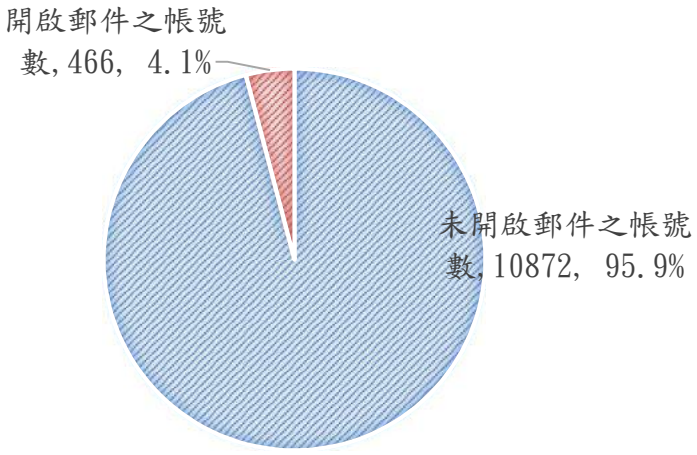


圖 8　開啟郵件帳號比例圖

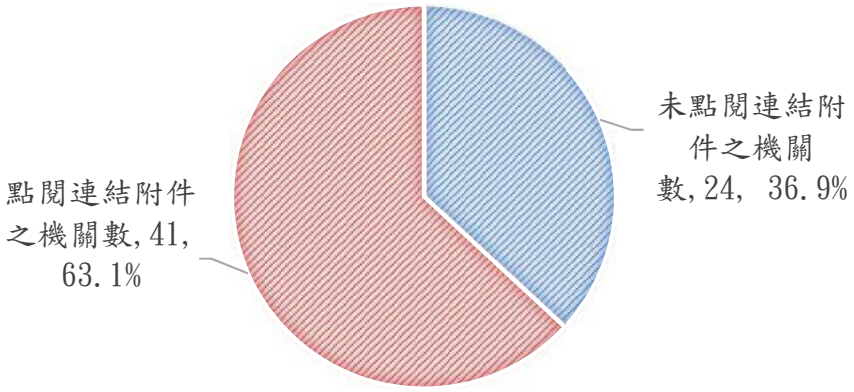


圖 9　點閱郵件連結/附件機關比例圖

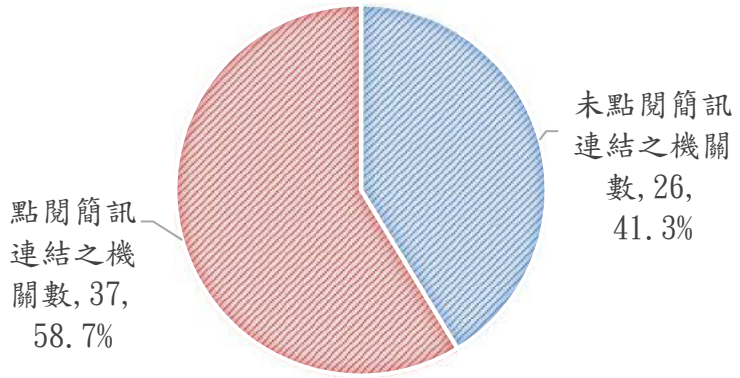


圖 10　點閱簡訊機關比例圖

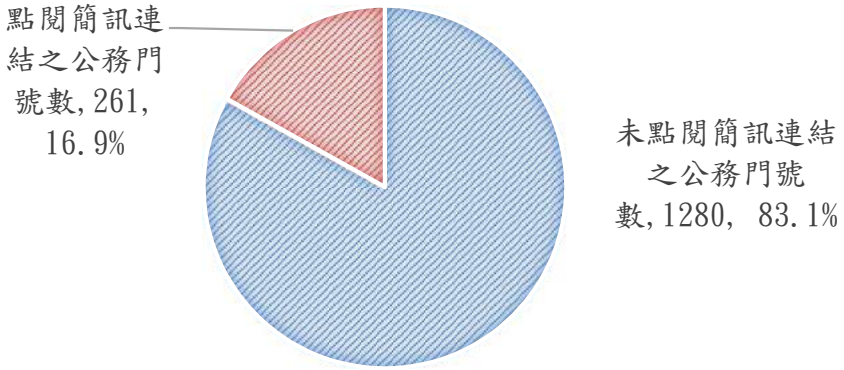


圖 11　點閱簡訊公務門號比例圖

四、資安稽核作業

為協助各機關強化資安防護工作之完整性與有效性，並持續精進以降低資安風險，爰辦理資安稽核作業，以外部角度協助機關檢視資安作業之落實情形，110 年遴選 11 個受稽機關，並彙整稽核發現資料，提出受稽機關建議改善事項及共同發現事項，供政府機關據以參考改進，以持續精進政府機關之資安防護水準，相關稽核發現說明如下：

(一)策略面

1. 部分機關資通安全維護計畫及實施情形填報內容有所差異，未有效界定核心業務及核心資通系統，且未以客觀與量化衡量指標評估系統防護需求等級。

2. 資通安全組織召開管審會議時，常有委員係代理出席情形，難彰顯管理階層之支持及重視。

3. 部分機關資通安全目標以資安事件發生次數為量測指標，考量資安目標妥適性，不宜納入資安事件發生次數。

(二)管理面

1. 資訊服務委外作業未於合約或建議書徵求文件明確規範防護基準需求，且未依法規要求落實，如委外廠商選任要求、防護基準納入建議書徵求文件、安全性檢測及通報程序等。

2. 資訊資產盤點作業，其盤點範圍與內容完整性不足，未包含全機關。

3. 部分機關辦理委外廠商稽核作業未記錄相關查核證據，且對稽核發現事項無建立追蹤管考機制。

4. 部分機關內部資通安全稽核作業，計畫內容不完整，應列出

稽核項目，並確認範圍之合宜性。

(三)技術面

1. 機關資通系統安全性檢測、滲透測試及資通安全健診等作業，未落實執行後續修補作業，應訂定相關作業程序辦理及追蹤。

2. 機關資通系統開發、測試、變更及上線等相關程序內容未臻完善，且未完整保留資通系統之版本更新過程與紀錄，另系統分析與設計文件未及時更新與納管。

3. 針對資通系統所使用之外部元件或軟體，缺乏明確管理規範。

五、政府機關資安事件通報

經彙整 110 年國家資通安全通報應變網站所接獲之政府機關通報資安事件共 696 件，其中 1 級事件為大宗占 86.19%，2 級事件為 11.44%，3 級事件為 2.37%，無 4 級事件，其事件影響等級比例圖詳見如下：

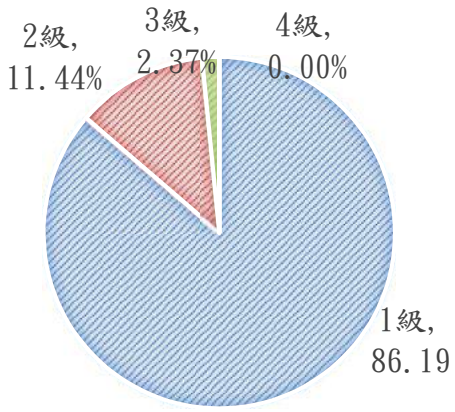


圖 12　110 年資安事件等級比例

分析 3 級事件以資料外洩事件居多，除網站設計不當或應用程式漏洞導致之外，近兩年皆發生使用 Google 表單蒐集民眾資料，因權限設定不當致使民眾可瀏覽他人填寫資料，造成個資外洩。

另，依通報之資安事件通報類型可分為非法入侵(63.32%)、設

備問題(12.19%)、網頁攻擊(4.10%)、阻斷服務(0.65%)及其他(19.74%)，經彙整110年政府機關資安事件通報類型比例詳見下圖：

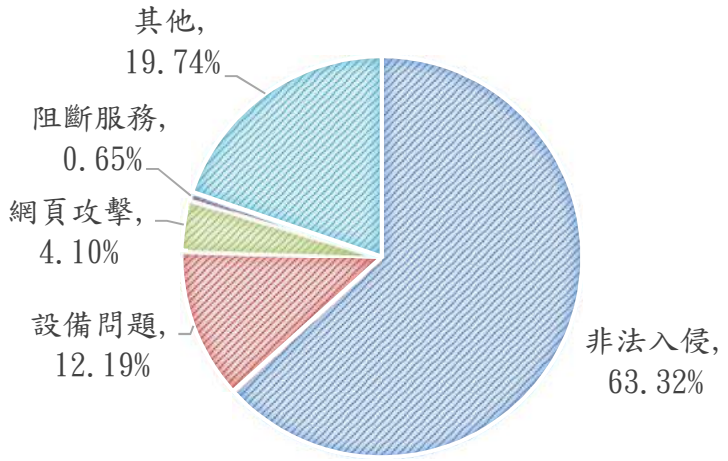


圖 13　110年政府機關通報類型比例圖

可明確辨識之資安事件類型以「非法入侵」事件居多，主要肇因係使用弱密碼或者廠商維運管理疏失等，相關案例包含委外廠商遠端連線未妥善管理，致遭駭客上傳惡意程式；或未遵循政府組態基準要求之複雜性與強度原則設定，導致帳號密碼遭暴力破解成功，並植入勒索軟體；或利用破解之郵件帳密大量寄送惡意郵件等。

「設備問題」為資訊設備未變更預設帳號密碼，其設備存在安全漏洞，遭駭客利用而成為攻擊目標，或設備異常、毀損等；「網頁攻擊」為網站設計不當，如未依循安全系統發展生命週期之機制，相關網站功能設計與設定疏失，致遭駭客上傳惡意程式，進而展開進階或橫向擴散攻擊。分析110年通報事件分布情形，中央機關占整體40.8%，地方機關則占59.2%。

肆、政府機關資安威脅情勢與防護建議

一、勒索軟體攻擊影響資料讀取

勒索軟體攻擊除將機關資料加密，導致受害者無法正常執行運作外，進而達到勒索贖金之目的外，更甚者，駭客將竊取與販賣機敏資料，實現第 2 次勒索。

相關事件案例為某機關發現數項資訊設備遭感染勒索軟體，致影響日常作業，遭駭後又擴散至核心資通系統，無法於可容忍中斷時間內回復正常運作，其業務影響重大；據調查結果，研判應係其設備維護廠商維運使用之帳號密碼遭駭客暴力破解，並利用該帳號登入維運設備後，再橫向擴散至其他設備。

建議委外廠商至現場進行維護，若需暫時開放遠端連線維護，至少應以白名單限制系統存取及鎖定來源 IP，維護廠商之系統帳號密碼亦應納入管理，並要求符合一定強度、定期更改密碼及加強系統錯誤登入嘗試次數設定等措施。另外，網路應建立適切之區隔與存取控制機制，並依資料分級原則限制存取或進行加密，以降低橫向擴散或外洩後風險。

二、物聯網與行動式設備疏於管理遭獲取系統控制權

惡意軟體持續活躍於物聯網殭屍網路，針對物聯網與網路設備漏洞發動進一步攻擊及入侵，常運用之手法為利用弱密碼、密碼暴力破解及應用程式漏洞等方式入侵。

110 年發現多個機關其物聯網設備存在下載惡意腳本之連線紀錄，例如某機關的監視器設備，因機關未變更監視器預設之帳號密碼，攻擊者即以預設帳密進入設備取得系統控制權。另一案例為某品牌多款雷射印表機、多功能事務機及掃描器存在之安全漏洞，攻擊者可向受影響設備傳送含有特製字型之惡意檔案，進而讓攻擊者可遠端執行任意程式碼。

建議各機關採購通過資安檢測之物聯網設備，並依據後續應用範圍，採取對應之資安防護措施；隨時注意原廠所提供之更新資訊，進行安全性測試及完成更新；此外，相關設備之網路連線應規劃網域區隔，進行連線行為監控與加強存取控制機制。

三、資訊服務供應商遭駭後影響機關業務

供應鏈攻擊最常見方式為駭侵機關委外之資訊服務供應商，將之成為攻擊政府機關的跳板，而委外人員(含業者駐點人員)之資安意識及未落實相關安全控制措施，經常成為資安防護脆弱之一環。

以某政府機關之資安事件為例，惡意攻擊者首先利用委外廠商維護機關系統所使用之遠端連線通道進行入侵，進一步使用勒索軟體加密機關資通系統，造成機關業務運作停頓；機關發現遭駭後，立即中斷主機網路連線，以避免橫向擴散，再透過系統備份重建受駭主機與系統，優先恢復業務正常運作，此類事件通常因駭客採取受信任管道入侵客戶網路，因此往往無法在第一時間發現。

建議各機關開放機關同仁及委外廠商進行遠端維護資通系統，應依本院資通安全處 110 年 3 月 2 日院臺護字第 1100165761 號函，以「原則禁止、例外允許」方式辦理，如允許外部遠端維護，應加強相關防護措施，包含事先要求申請開放短天期之維護時間、限制特定存取來源位址及採用多因子驗證等方式，並監控相關活動，同時要求委外廠商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。

四、進階持續性威脅攻擊尋找入侵點

進階持續性威脅攻擊通常是具備組織性及目的性之長期潛伏攻擊活動，攻擊者鎖定特定組織，針對資通訊統或網路設備之弱點，找出可進入之入侵點。

110 年發生有駭客重製政府機關網站之公告訊息,偽造為釣魚郵件，針對特定機關發動魚叉式社交工程攻擊，經分析該釣魚郵件之附檔為內嵌巨集程式碼與惡意程式之簡報檔，當收件人點選附檔、啟動巨集後，即會將惡意程式植入到收件人電腦，並連線中繼站下載第 2 階段惡意程式。在其他案例亦發現駭客以請求政府機關業務辦理窗口協助為由，針對特定機關發動 APT 惡意電子郵件攻擊，以夾帶含有個資之壓縮檔，誘使收件者輸入郵件內文中之密碼開啟後執行惡意程式，此類攻擊者使用含有密碼之壓縮檔做為附件，亦顯示其欲規避防護設備檢測之企圖。此外，針對駭客電子郵件附檔惡意程式攻擊，以微軟 Office 文件系列之遠端執行漏洞(CVE-2017-11882)最多，占整體 45.4%，該漏洞容易觸發且適用平台廣泛，自 106 年揭露至今仍是惡意文件附檔攻擊最常利用之漏洞。

建議各機關應強化人員資安意識，注意郵件來源之正確性，不開啟不明來源郵件與附檔，將相關日誌納入監控機制，檢視是否存在異常連線行為，並評估將受駭偵測指標部署至機關資安監控防護機制，以偵測是否有相關異常連線行為。

五、社交工程詐騙方式詭譎多變

近年發現駭客大量利用疫情或重要投資資訊等內容製作詐騙與勒索郵件，並夾帶惡意郵件附檔誘騙使用者開啓並連線，其附檔多為遠端木馬惡意程式，相較於 109 年社交工程之駭侵手法，其惡意電郵附檔從「殭屍網路」、「勒索軟體」，於 110 年攻擊趨勢有轉向散布「遠端木馬」惡意程式之情形。

110 年資安事件案例為駭客透過社交工程郵件夾帶惡意文件檔案，企圖誘騙收件人開啟惡意程式以竊取受駭者電腦資訊，有別以往駭客使用含 VBA 巨集之 XLM 惡意文件檔案進行攻擊，此次駭客使用 Excel 擴充外掛之 XLL 檔案，攻擊者可利用檔案在受駭電腦端

執行各種惡意行為並下載進階後門程式，藉以蒐集資訊並回傳到駭客伺服器。另外有多個機關電子郵件帳號遭到暴力破解，駭客成功登入郵件伺服器後，蒐集相關郵件帳號與密碼資訊，進而利用破解之帳密大量寄送社交工程釣魚郵件郵件，經分析發現遭入侵成功之系統，多為無限制外部存取與提供網頁登入之郵件伺服器；其他事件案例亦發現駭客利用免費網站架設平台(Weebly)與線上表單服務平台(Wufoo)建立釣魚網站，並寄送社交工程釣魚郵件，由於該免費平台因操作介面簡單，無需具備程式設計能力即可架設網站，廣受大眾喜愛，因此藉由該平台駭客易於騙取政府機關人員帳號密碼。

建議機關應定期進行郵件伺服器漏洞修補，並設定伺服器錯誤登入嘗試次數，以降低暴力破解可能性；此外，建議評估納入多因子驗證之登入機制，並定期變更密碼。

伍、結語

經檢視 110 年國內資安威脅情資發現，勒索軟體攻擊影響資料讀取、物聯網與行動式設備疏於管理、資訊服務供應商遭駭、進階持續性威脅攻擊及社交工程詐騙等項，仍為政府機關當前重要之資安防護議題；考量我國政經情勢特殊，除面對全球複雜多元之資通訊變革，尚需面對較其他國家更為險峻之資安威脅，因此持續落實精進各項資安防護工作，實屬必要。本院於 110 年發布「國家資通安全發展方案(110 年至 113 年)」，將持續推動國家資安整體發展策略，建立國家資安聯防體系，提供事前安全防護、事中緊急應變、事後復原鑑識等資安技術服務，協助機關強化資通安全防護能量，建立主動防禦機制，降低資安風險，以打造安全可信賴之數位國家。