國家資通安全情勢報告

行政院

中華民國 108 年 6 月

目次

壹、依據及目的

資通安全管理法(以下簡稱資安法)於 107 年 5 月 11 日經立法院三讀通過，並於 108 年 1 月 1 日正式施行，本院依據資安法第 5 條規定，公布「國家資通安全情勢報告」。

本報告以 107 年政府機關及國際間之資通安全威脅情勢研析結果，作為本報告之主軸，供各政府機關作為精進資安防護作為之參據，本報告後續將定期更新公布，並增納關鍵基礎設施之資安情勢，本院期望藉由本報告之公布，除讓各界了解公部門所面臨之資安威脅外，亦期能提升各界之資安意識，透過公私協力，共同提升國家整體資安防護能量。

貳、107 年全球資安威脅情勢概要

根據世界經濟論壇(World Economic Forum，簡稱 WEF)「2018 年全球風險報告」[1]指出，在科技風險類別中，「網路攻擊」、「資料欺詐或盜竊」及「關鍵基礎設施中斷」之風險逐年升高，而網路攻擊與資料欺詐或盜竊之風險更分別高居全球發生機率前 3 名與 4 名。另外，在國際知名網路公司之 107 年度網路安全報告[2]中亦指出，「惡意人士越來越擅長規避，並且運用雲端服務及其他合法用途之技術做為他們的武器」、「欠缺安全防護及不斷擴增的物聯網(Internet of Things，簡稱 IoT)及雲端服務，已成為有心人士利用之攻擊工具」。

從 107 年全球資安事件研析發現，網路攻擊朝多樣化演變，除了分散式阻斷服務(Distributed Denial of Service，簡稱 DDoS)攻擊癱瘓網路服務之事件仍持續發生外，隨著物聯網 IoT 設備的普及，針對其攻擊之數量亦隨之增加。此外，現今駭客已發展成集團式組織，且有目標式的鎖定特定對象持續展開入侵活動，駭客目的除在獲取金錢利益外，龐大的個人資料竊取商機亦為駭客所覬覦。另一個不可忽視的現象是針對關鍵基礎設施攻擊，關鍵基礎設施一旦遭駭，對社會秩序、民眾安全產生巨大影響，以下綜整 107 年全球重大網路攻擊事件如圖 1，並說明如下：

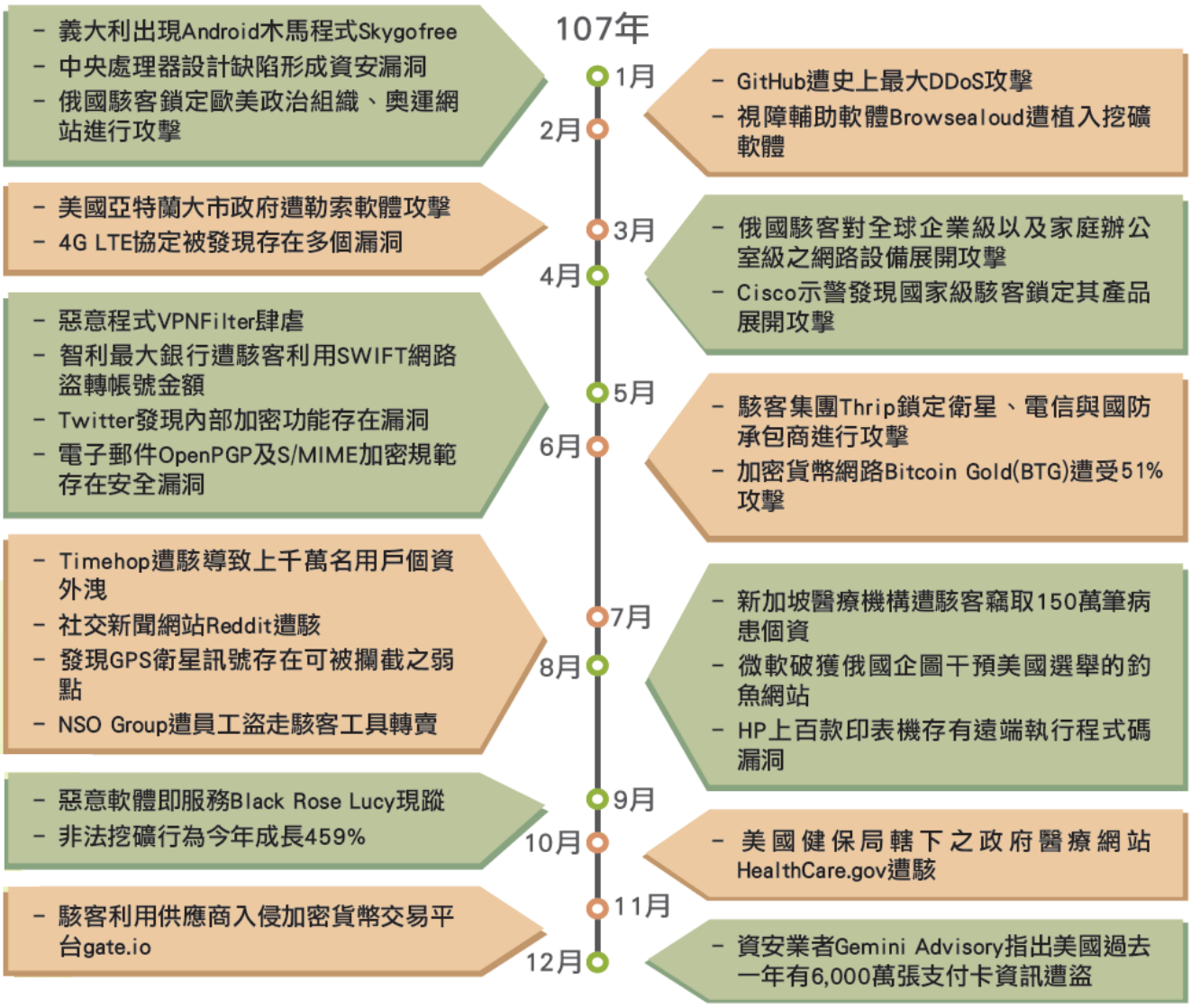


圖 1 107 年全球重大網路攻擊事件

一、藉由 APT 攻擊竊取機敏資料

隨著個人社群媒體及雲端服務之興起，當個人享受前述服務之便時，有心人士也順勢利用這些服務，進行所謂「進階持續性威脅(Advanced Persistent Threat，簡稱 APT) 攻擊」，造成民眾個資及企業業務敏感資料外洩，以下就雲端服務廠商 Timehop 遭 APT 攻擊，以及資安業者 McAfee 揭露之駭客「神槍手行動(Operation Sharpshooter)」等 2 項案例，進一步剖析相關攻擊手法。

Timehop 為 Facebook、Twitter 及 Instagram 等社群網站提供貼文回顧服務，106 年起 Timehop 遭駭客採取 APT 攻擊，竊取了管理員帳密，後續駭客連續於 106 年 12 月、107 年 3 月及 6 月先後登入其雲端服務進行環境偵查，隨後在 107 年 7 月 4 日開始攻擊 Timehop 主要資料庫，並對外傳輸資料，該事件導致 2,100 萬用戶個資外洩。

第 2 起案例為資安業者 McAfee 於 107 年 12 月 12 日揭露之「神槍手行動」網路攻擊，該行動駭客鎖定各國重大建設，從核子、國防、能源到金融組織進行攻擊，至今已於 24 個國家、87 個組織發現該行動駭客的蹤跡。根據 McAfee 的分析，「神槍手行動」採取之 APT 攻擊步驟，先是利用 Dropbox 散布惡意的 Word 文件，當文件後續被下載及開啟，即於 Word 記憶體中植入簡易木馬程式，該木馬程式會蒐集電腦上的資訊並傳送至由駭客控制的命令與控制(Command and Control，簡稱 C&C) 伺服器，隨之再由 C&C 伺服器傳送完整的惡意模組 Rising Sun 到受害者電腦上，Rising Sun 可用來執行命令、取得磁碟資訊、執行各種程序、讀取檔案、清除程序記憶體、將檔案寫入磁碟、刪除檔案或取得檔案的額外資訊等。

二、透由 DDoS 攻擊癱瘓網路運作

藉由干擾組織之網路服務運作，使組織與使用者不安的狀況下，繳

交贖金，而分散式阻斷服務攻擊（DDoS）即為近年來有心人士常用之手法之一，目標常以金融、資訊科技及雲端服務等組織為主，以下就原始碼代管服務之軟體開發公司 GitHub 遭到該類攻擊之案例進行說明。

107 年 2 月 GitHub 公司發現網路異常流量後，即面對源自於數萬個端點自治系統(Autonomous System，簡稱 AS)，以每秒傳送約 1.27 億個封包，尖峰流量達到 1.35 Tbps 之目前史上最大的 DDoS 攻擊。GitHub 在事件發生當下，發現輸入流量與輸出流量有著顯著的差異，且在輸入流量超過 100 Gbps 後，雖嘗試將流量導至雲端服務平台 Akamai 公司，希望透由 Akamai 公司的資源來擴充邊緣網路容量，但突如其來的流量仍讓 GitHub.com 一度斷線，且之後仍發生間歇性斷線的情況。駭客在第一波攻擊後，持續展開波段攻擊，據網路安全業者 ThousandEyes 指出，鎖定 GitHub 的 DDoS 攻擊並未就此結束，107 年 3 月又觀察到 GitHub 遭到另一波大規模攻擊，而且可用性下滑至 61%，儘管遭到輪番攻擊，但 GitHub 強調用戶資料並未受到波及，且正在研究如何強化邊緣架構與自動化緩解能力。

三、IoT 設備資安弱點威脅升高

根據 WEF「2018 年全球風險報告」[1]指出，IoT 設備在 106 年已達 84 億台，預測在 109 年會增加到 204 億台設備，而 OWASP(Open Web Application Security Project)資安組織，也提出了十大 IoT 的弱點，提醒廠商及使用者應以面對網站應用系統威脅的態度，正視 IoT 裝置帶來的威脅弱點，以下即以駭客組織利用「少爺殭屍網路」攻擊家用路由器，以及網路設備商 MikroTik 遭駭之案例說明。

組織型駭客利用「少爺殭屍網路」，透由社交工程手段，誘騙路由器連網使用者下載惡意程式，以達竊取個人資料之目的，截至 107 年 4 月，已有 20 多萬台路由器被駭客掌控，至少 6,000 台行動裝置遭感染，

該應用程式不僅能取得手機型號、作業版本、系統及應用程式列表等資訊，還能竊取受害者的帳號、聯絡人資料及簡訊內容，並可遠端撥號、接收及寄送簡訊，其造成個人資料外洩估計超過 100 萬筆，且感染範圍擴及全球 55 個國家。

另外，歐洲拉脫維亞(Latvijas)知名網路設備公司 MikroTik 遭駭客攻擊事件，該公司商品包括路由器與相關網通設備，市占率為 2.8%，但駭客透過 MikroTik 路由器之漏洞(CVE-2018-14847 與 CVE-2018-1156)，入侵受害設備並取得 Root Shell 權限，以竊取受害設備之相關資訊。依據 108 年 1 月 14 日 Shodan 統計資料，MikroTik 在全球的使用量共 1,879,520 台，排名前 5 名之使用國家分別為巴西(250,129 台)、中國(190,830 台)、印尼(142,513 台)、俄羅斯(134,837 台)及伊朗(91,722 台)，MikroTik 在我國的使用量則有 13,156 台，故當全球知名 IoT 設備一旦傳出災情，受害者將遍及全球。

四、工業控制系統受攻擊風險倍增

根據 WEF「2018 年全球風險報告」[1]指出，除網路攻擊的風險排行一直居高不下外，另一個值得觀察的重點是在科技風險類別排名第 2「關鍵基礎設施因其工業控制系統遭受攻擊而服務中斷」，下述以惡意程式 VPNFilter 攻擊特定的工業控制系統，以及美國政府武器系統遭駭侵之案例說明。

網路設備公司 Cisco 旗下的 Talos 安全部門於 107 年 5 月 23 日發現，駭客利用已感染模組化惡意程式 VPNFilter 之網路裝置，攻擊特定的工業控制系統，尤其是資料蒐集與監控系統(Supervisory Control And Data Acquisition，簡稱 SCADA)協定之工業控制系統，它能監控裝置流量，竊取網站憑證，還能切斷裝置的連網能力或讓裝置無法使用，此惡意程式共感染 Linksys、MikroTik、NETGEAR 及 TP-Link 及 QNAP 之

網路儲存裝置(Network Attached Storage，簡稱 NAS)。VPNFilter 主要分為 3 個攻擊階段，首先是登入裝置並與遠端命令暨控制(C&C)伺服器建立連線，再來是自 C&C 伺服器下載可蒐集裝置資訊及破壞裝置能力的模組，最後則是下載能監控裝置流量及竊取網站憑證的模組，經調查發現，即便使用者重新開啟這些被駭的裝置，也只能移除第 2 與第 3 階段的模組，第 1 階段的 VPNFilter 元件仍會持續存在，僅能透過恢復原廠預設值才能移除它。目前遭 VPNFilter 鎖定的國家是烏克蘭，但它仍然感染全球 54 個國家的路由器或 NAS 裝置，再加上它的感染規模達到 50 萬台，讓美國聯邦調查局(Federal Bureau of Investigation，簡稱 FBI)近期成功取得美國法院的命令，要求域名管理公司 VERISIGN 把駭客所使用的 ToKnowAll.com 網域名稱轉交給 FBI，切斷駭客與這些被駭裝置的聯繫管道，以阻止一場可能發生的資安災難。

另外，美國政府課責署(Government Accountability Office，簡稱 GAO)於 107 年針對美國國防部(Department of Defense，簡稱 DOD)的武器系統發表一篇滲透研究報告[3]指出，DOD 主要武器系統缺乏嚴密的安全機制，只要利用簡單的工具及技術，就能在不被察覺的情況下掌控相關系統。尤其是 GAO 針對 DOD 各式武器系統展開滲透測試發現，某組測試團隊只花 1 個小時就入侵其中一個武器系統，接著用 1 天時間取得該武器系統的完整控制權。

五、網路經濟罪犯影響電子商務與金融運作

根據防毒軟體公司趨勢科技在 108 年資安預測報告[4]指出，與網路釣魚相關而被阻隔的惡意網址數，從 106 年的 7,300 多萬大幅度成長至 2 億 1,000 多萬；值得關注的是，這些網路釣魚的網址或連結，不僅來自於電子郵件，亦存在於手機訊息與即時通訊，而駭客則利用此駭侵管道染指電子商務及金融業，以詐騙或勒索金錢，以下就智利最大銀行

Banco de Chile 遭惡意程式入侵之案例說明。

107 年 5 月 Banco de Chile 遭網路釣魚手法植入惡意程式，計有逾 9,000 台員工電腦及 500 台伺服器無法開機，駭客更企圖趁亂利用環球銀行金融電信協會(Society for Worldwide Interbank Financial Telecommunication，簡稱 SWIFT)網路盜轉銀行金錢，智利銀行於 107 年 5 月 24 日首先發布公告，表示偵測到 1 個影響分行與電話銀行等服務的「瑕疵」，但表示其他服務正常運作。不過隨後在 5 月 28 日承認，遭到來自網際網路的病毒感染，直接影響該銀行主管及櫃台人員的工作站，導致分行與電話銀行服務無法運作，後續智利銀行即啟動緊急應變措施，切斷工作站與其他作業系統之連結，以防止病毒擴散。

六、資通產品服務廠商遭駭破壞供應鏈安全

美國國家標準技術研究所(National Institute of Standards and Technology，簡稱 NIST)[5]，在 107 年 4 月更新其網路安全框架時，特別將「供應鏈風險管理(Supply Chain Risk Management，簡稱 SCRM)」增列至核心類別，代表在現今與未來的網路世界中，供應鏈之風險已有相當重要性且需全面識別與因應。隨著雲端服務、人工智慧及 IoT 等新興科技的崛起，供應鏈範圍不僅是一般傳統的供應商，還包括其他外部連網元件或通訊等供應商，如何管理供應商或了解相關風險變得更具挑戰性。以下就網站流量分析服務供應商 StatCounter，存在漏洞遭駭客入侵之案例進行說明。

資安業者 ESET 於 107 年 11 月 6 日報告指出，駭客於 StatCounter 網頁植入惡意的 JavaScript，當各家網站利用 StatCounter 分析網路流量時，駭客即可追蹤訪客網頁上嵌入之 JavaScript，並注入惡意程式。經發現，駭客主要瞄準比特幣之交易網頁，並自動將受害者之轉帳位址改為駭客所掌控的貨幣錢包，造成重大損失，經查 gate.io 已在官網宣佈將停用 StatCounter 的服務[6]。

參、107 年政府資安威脅統計

一、政府機關資安事件通報

107 年政府機關通報之資安事件數量計 754 件，各級資安事件依嚴重等級低至高共分 4 級[7]，各級資安事件發生件數及比例如圖 2 及圖 3：

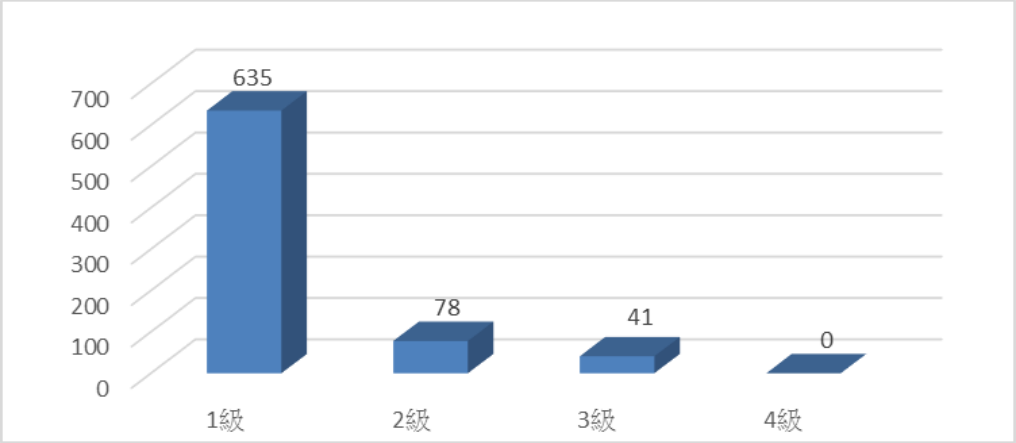
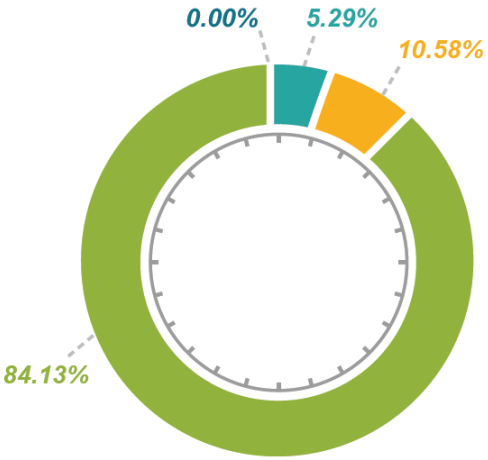


圖 2 107 年各級資安事件通報數量



備註：依事件造成之機密性、完整性及可用性衝擊之嚴重度區分，由輕至重分為「1 級」、「2 級」、「3 級」及「4 級」

圖 3 107 年各級資安事件通報比例

各資安事件發生原因之分布情形如圖 4，主要發生原因說明如下：

(一) 網站設計不當：因自行開發或委外開發網站時，未遵循安全系統

開發流程，致未經安全檢測之程式上線使用，而遭駭客利用，107年發生比例為24.35%。

(二) 應用程式漏洞：部分政府機關網站，因未即時更新第三方元件，造成安全性漏洞，107年發生比例為11.91%。

(三) 弱密碼:部分政府機關之網站管理後台或郵件系統等登入帳號，使用弱密碼或是預設密碼，並遭有心人士成功猜測、破解而入侵利用；或因遠端服務開放匿名存取功能，未限制存取來源與權限等安全性漏洞遭植入挖礦程式,107年發生比例為11.52%。

(四) 其他：發生比例為32.59%居首，多數係因部分機關日誌保存不足、人力受限、系統設定等因素，致事件根因追蹤不易。

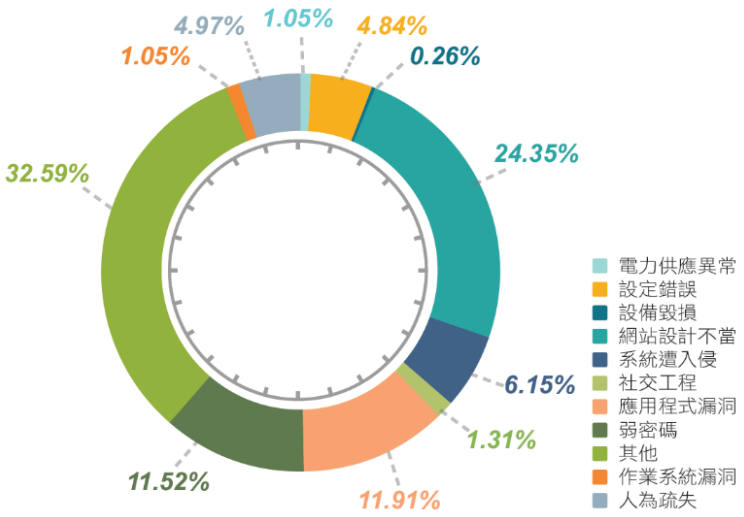


圖 4 107年資安事件發生原因分布

二、資安攻防演練

本院為提升政府機關在面對網路攻擊之應處能力，每年針對政府機關辦理網路攻防演練，演練內容包括資訊系統實兵演練及社交工程演練，107年演練結果如下：

(一)資訊系統實兵演練

107年實兵演練共64.62%政府機關遭演練攻擊成功,所發現之弱

點區分為高衝擊性、低衝擊性及 Info 衝擊性等 3 類，各類弱點衝擊性分布情形如圖 5，說明如下：

1. 高衝擊性弱點：以無效的身分認證與機敏資料外洩最為常見，占 34.89%。
2. 低衝擊性弱點：以跨網站腳本攻擊為主，占 47.32%。
3. Info 衝擊性弱點：以錯誤的安全性設定為主，占 17.79%。

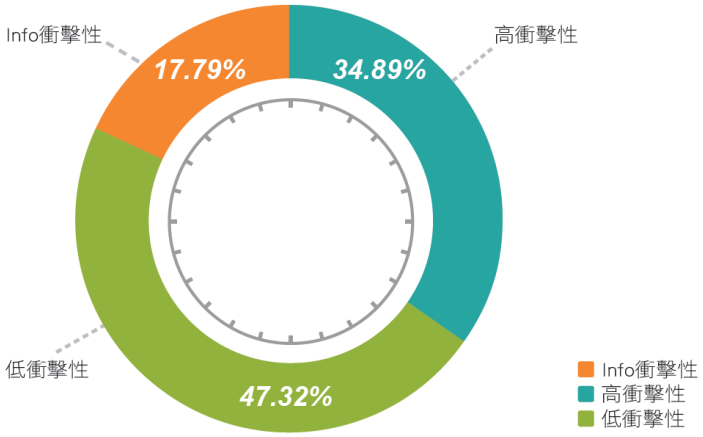


圖 5 各類弱點衝擊性比率圖

進一步分析弱點類型，107 年實兵演練所發現之弱點涵蓋 10 種弱點類型，其中以「不安全的組態設定」與「跨網站腳本攻擊」比率較高，分別占 31.43%與 19.17%，詳見圖 6。

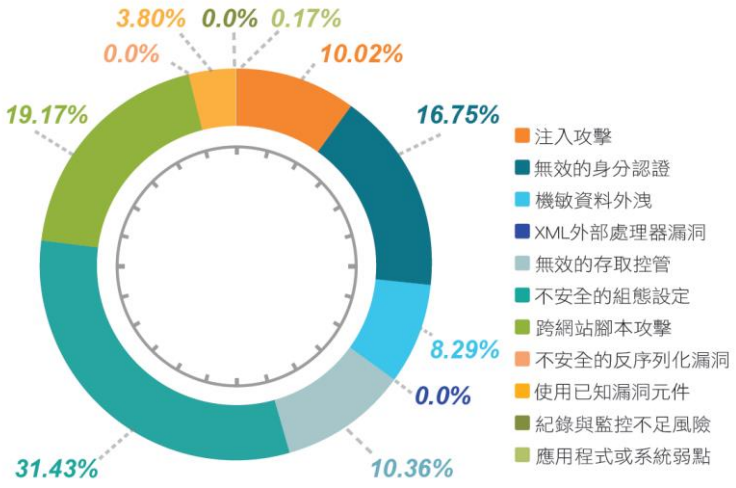


圖 6 弱點類別分布比率圖

(二) 社交工程演練

以電子郵件及簡訊方式進行 65 個政府機關之社交工程演練，測試機關對於社交工程攻擊之資安意識與警覺性。

107 年開啟郵件及點閱附件或連結之平均比率分別為 4.74%與 3.01%，詳見圖 7 與圖 8；另開啟簡訊附件或連結之機關比率為 27.93%，詳見圖 9。

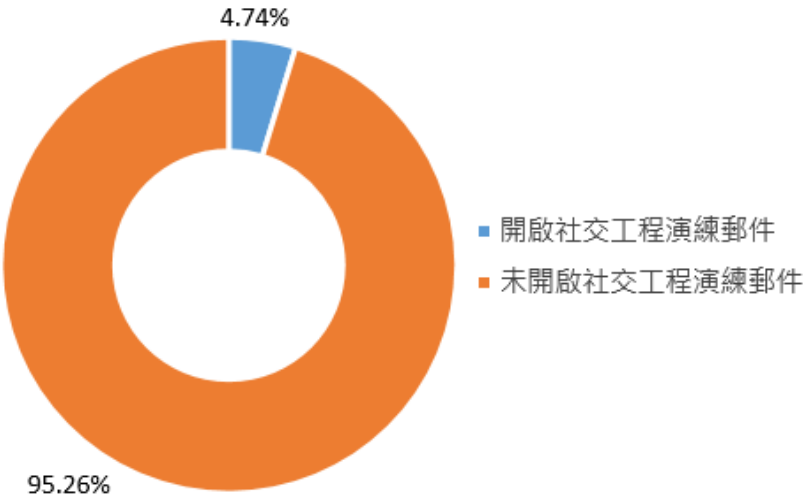


圖 7 開啟郵件之平均比率圖

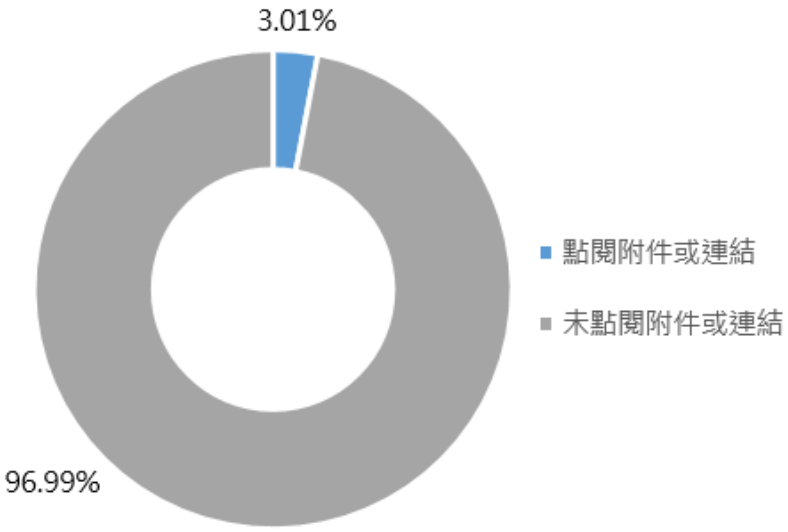


圖 8 點閱附件或連結之平均比率圖

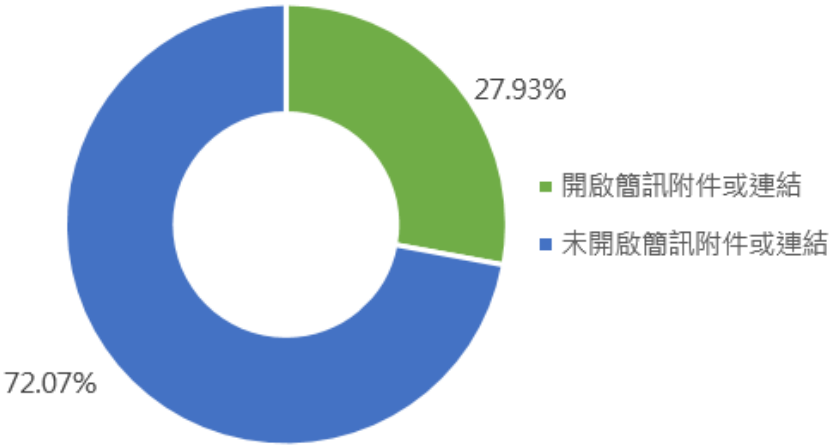


圖 9 開啟簡訊附件或連結之平均比率圖

三、資安稽核作業

為協助政府機關提升資安防護之完整性及有效性，本院每年挑選重要機關辦理資通安全稽核作業，稽核作業分實地稽核與技術檢測作業，107 年計完成 25 個機關之稽核作業，辦理情形如下：

(一) 實地稽核

實地稽核內容涵蓋「策略面」之導入資訊安全管理系統範圍適切性、機關首長對資安業務支持度、資源投入資安業務狀況、資安業務運作規劃與落實；「管理面」之個人資料保護與管理、資產管理與風險評鑑、人力資源管理、資訊委外安全管理，以及「技術面」之通訊與作業安全、資安事件通報與處理及資通系統開發與維護安全等 11 個稽核項目進行，107 年 25 個機關實地稽核成績分布如圖 10，其中 8 個機關表現良好，成績達 75 分以上。

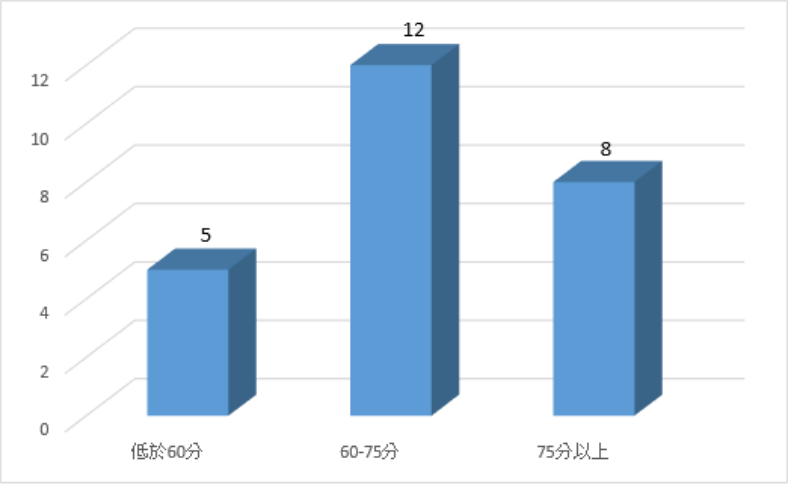


圖 10 107 年實地稽核整體平均分數

(二) 技術檢測

技術檢項目包括「使用者電腦弱點掃描」、「惡意中繼站連線阻擋檢測」、「核心資通系統安全檢測」、「網路架構檢測」及「活動目錄(Active Directory，簡稱 AD)主機安全防護檢測」5 大項，25 個機關之技術檢測成績平均分數 65.81 分，詳見圖 11，其中 6 個機關表現良好，成績達 75 分以上者。

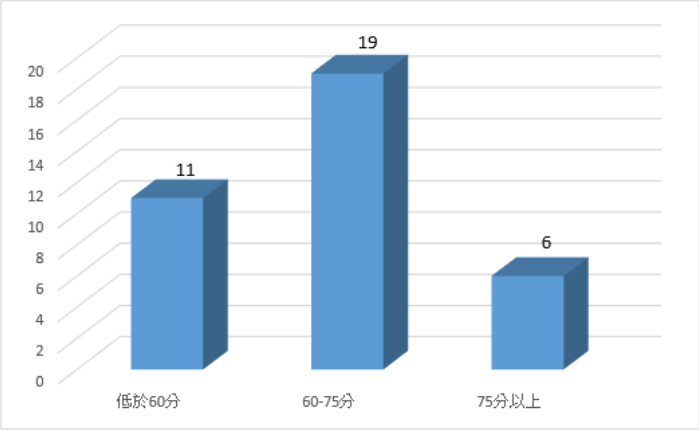


圖 11 107 年技術檢測整體平均分數

(三) 資安稽核共同發現事項

1. 策略面

(1) 資安推動組織之參與度待提升，應加強機關所有單位共同參與 ISMS 作業。

(2) 管理審查之執行與後續改善追蹤等項仍需加強落實，包括與會人員與討論項目等，且後續改善追蹤應確實並留下紀錄。

(3) 核心資通系統鑑別、資產風險評估及業務營運衝擊分析等結果欠缺關聯性。

(4) 異地資料備份/備援機制宜強化規劃與落實，確保資料與系統之可用性。

2. 管理面

(1) 亟待建立完整的個人資料管理制度 (包括個人資料盤點、風險評估、隱私衝擊分析及相關管理等)。

(2) 亟待強化對委外廠商之資安要求及有效監督與管理，包括委外廠商管理程序、契約要求、駐點人員管理及資安稽核等。

(3) 資訊安全管理系統(Information Security Management System，簡稱 ISMS)文件與相關法規/規範要求不一致，應檢視 ISMS 相關文件。

3. 技術面

(1) 存取權限控管與遠端存取安全尚待加強。

(2) 亟待強化安全系統發展生命週期(Security Systems Development Life Cycle，簡稱 SSDLC)防護規劃與落實。

(3) 資通安全事件通報機制，程序、政策規定與實際作法不一致。

(4) 使用者電腦未落實相關安全管控及安全更新等作業。

(5) 亟待強化 IoT 設備盤點及相關安全防護。

四、聯防預警情資

為整體掌握政府機關資安潛在威脅，國家資訊安全防護中心(簡稱 N-SOC)定期彙整政府機關資安預警情資與事件，掌握資安威脅類別及趨勢。經分析 107 年所彙整之情資，計分為系統服務、入侵攻擊、阻斷服務、惡意程式、政策規則、掃描刺探及尚需調查等 7 類，其中前 3 名分別為入侵攻擊類(占 40.38%)、掃描刺探類(占 36.09%)及惡意程式類(占 6.14%)，各類威脅分布情形詳見圖 12。

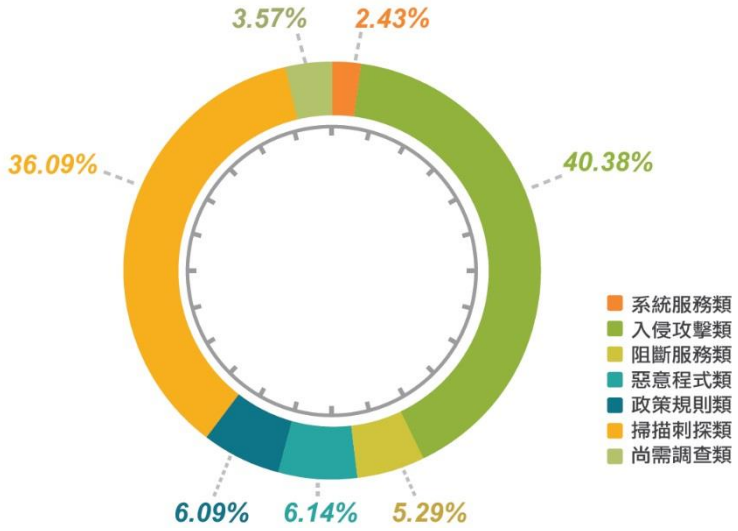


圖 12 資安威脅類別比率圖

五、惡意電子郵件

107 年觀察針對政府機關之電子郵件社交攻擊趨勢，其攻擊數量雖較 106 年下降（如圖 13），惟發現 11 月選舉期間之惡意電子郵件數量暴增，詳見圖 14，經檢測附件夾帶惡意檔案係以 Office 文件類型為主。

另外發現惡意電子郵件進行攻擊來自組織型駭客，且以鎖定特定目標以針對性(Targeted)方式進行攻擊，106 與 107 年 APT 惡意電子郵件攻擊類型詳見圖 15。

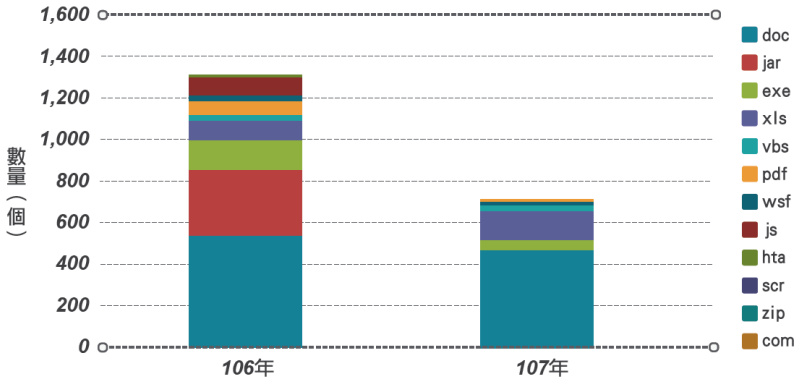


圖 13 惡意檔案數量與類型

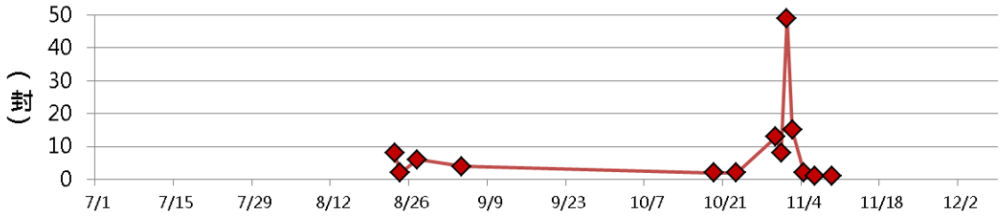


圖 14 107 年 7 月至 12 月惡意電子郵件數量

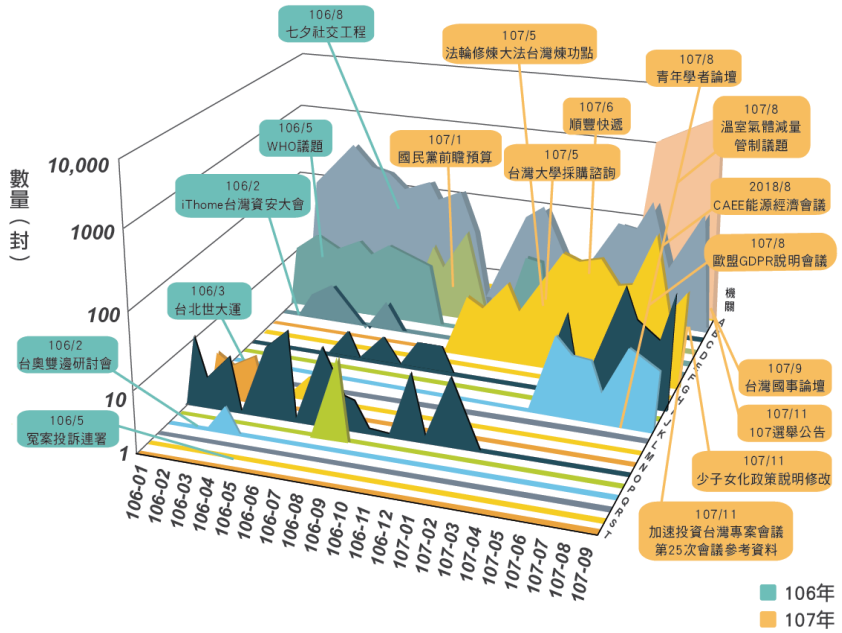


圖 15　惡意電子郵件類型

六、僵屍網路趨勢

107 年經由內外部情資所蒐集之惡意程式樣本中，發現 MIRAI 殭屍網路族群的攻擊次數高達 1 億多次，攻擊次數最多的前 5 大 MIRAI

變種類型包括 VIRIA、OWARI、AK1K2、SORA 及 ECCHI，占全體攻擊比率約 61%，詳見圖 16。

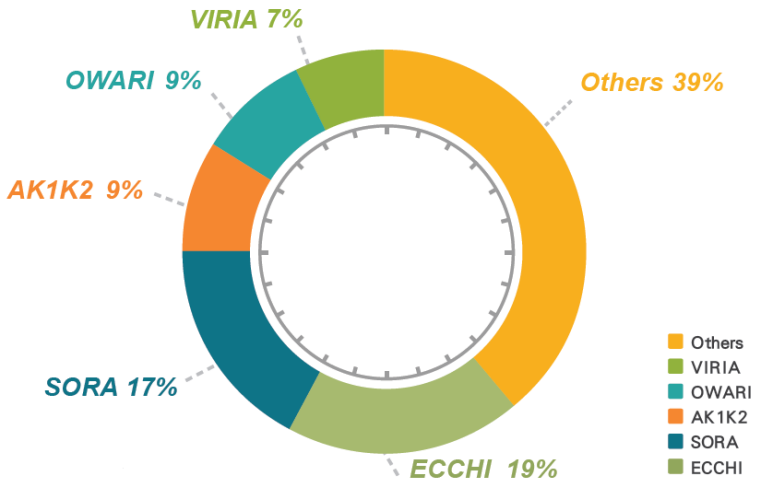


圖 16 MIRAI 殭屍網路族群攻擊之變種類型比率圖

MIRAI 主要攻擊目標為家用路由器及網路監控器等 IoT 裝置，目前仍有持續散布與感染各種 IoT 設備的趨勢，為不可忽視之威脅。

107 年共分析出 2,500 筆新的樣本程式，比 106 年的 2,343 筆多出 157 筆新的樣本程式，顯示惡意程式快速變種與多樣化，每月分析出之惡意程式數量，詳見圖 17。此外，107 年共偵測出 1,608 筆惡意程式連線惡意 URL，透過 URL 來進行程式自主更新、指令下載及回報，藉此規避防火牆與入侵偵測系統的偵測，提升殭屍網路活動與入侵的成功率，已為常見攻擊手法。

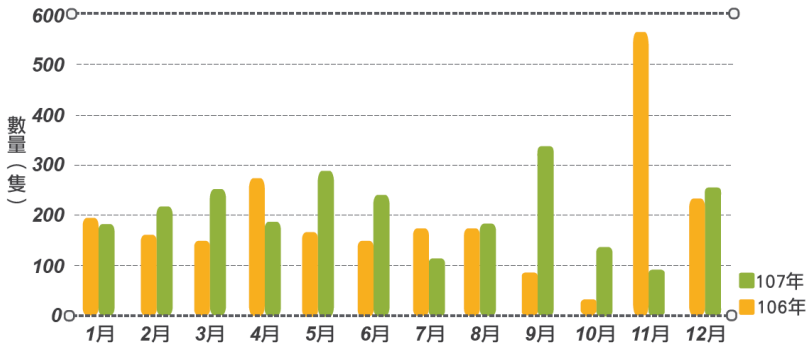


圖 17 107 年 1 月至 12 月每月殭屍網路惡意程式數量

肆、政府機關資安威脅情勢

經綜整前節之 107 年國內外資安威脅情資，歸納政府機關面臨之資安威脅如下：

一、特殊活動期間社交郵件攻擊頻密

惡意電郵攻擊長久以來一直是政府機關面臨的主要資安威脅之一，駭客利用夾帶惡意文件與檔案之電子郵件，如社交工程、釣魚信件及垃圾郵件等，透過公務或時事相關主旨誘騙目標使用者開啟惡意文件，使得目標電腦陷入被惡意程式感染控制之威脅，進而導致機敏公務資料外洩風險提高。

分析 107 年度政府機關遭惡意電郵攻擊之趨勢發現，11 月份攻擊郵件數量遽增，惡意電子郵件攻擊數量為全年度最高，主要以資通安全責任等級 A 級機關為主要攻擊目標，且駭客從 8 月下旬開始寄送惡意郵件，10 月底至 11 月初針對蒐集到的攻擊目標帳號，客製化相關業務信件與誘餌文件，並發動大規模社交工程郵件攻擊，經研判為當時適逢九合一大選期間，有心人士認為此為結合時事議題以獲較高攻擊成功機會之最佳時機。

二、挖礦程式興起

隨著加密貨幣與區塊鍊的熱潮，近年來駭客多利用使用者系統相關弱點，埋入挖礦程式，以偷取使用者電腦資源，協助其「挖礦」賺取虛擬貨幣，此威脅容易導致使用者系統變慢、效能不彰。

107 年政府機關間亦發生若干案例，例如：公車站電子看板，存在 Root Bridge 而遭植入挖礦程式、伺服器遭利用 Apache Structs2 及作業系統漏洞進行攻擊，植入門羅幣挖礦程式等。由此可知，除駭客過去常用以勒索軟體賺取金錢之手法外，挖礦程式亦為其另闢生財之道，各政府機關需加強防範。

三、工業控制系統發現入侵案例

一般而言，政府機關自行維運之工業控制系統仍屬少數，多數仍以提供網路服務之資通系統為主，惟 107 年出現攻擊政府機關內部機房環控系統之少見案例；駭客入侵該系統，取得調整濕度、空調及電磁脈衝設備設定調整之權限，藉此影響資訊機房運作（如圖 18）。

分析本案例發生原因，多因機關未限制系統存取權限，且對外開放網際網路存取，暴露遭駭客入侵並植入惡意程式之威脅弱點所致。

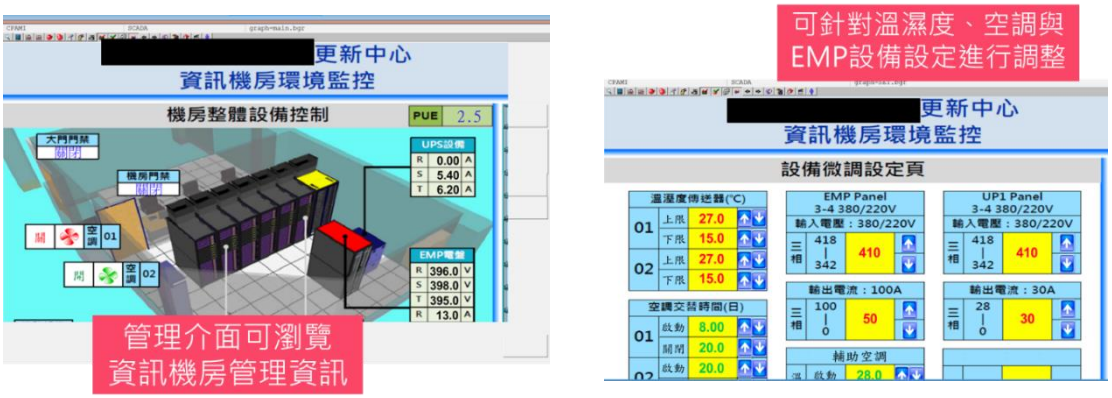


圖 18 環境控制系統入侵案例

四、資通系統委外供應鏈攻擊嚴重

近年來全球發生多起供應鏈遭受攻擊事件，駭客藉由入侵攻擊目標上下游供應鏈中最薄弱的環節，將惡意程式利用該受信任的管道進行散播，間接入侵目標。

107 年發生數起政府機關委外資訊供應商遭駭事件，導致機關所持有之敏感資料外洩，該類事件係駭客利用供應商開發之委外系統漏洞或開放委外廠商遠端連線之測試機，因存取權限設置不當而遭進行攻擊。

分析此類事件根因，多為資安(訊)供應商之資安管理完備度未盡嚴謹，且政府機關疏於監督管理所致。

五、IoT 設備威脅升高

近年來，由於 IoT 設備數量增長快速且種類多元，加上安全防護措施不足，常被駭客入侵後作為發動 DDoS、惡意中繼站之工具，相關案例數量逐年升高。入侵目標除了家用路由器及網路監控器之外，同時也有散布與感染至其他 IoT 設備類型之趨勢。

以 107 年發現之「少爺殭屍網路」為例，駭客透過入侵家用路由器，誘騙利用該路由器連網之使用者下載惡意應用程式(Application，簡稱 APP)，以達竊取個人資料之目的，至少 20 多萬台路由器被駭客掌控，6,000 台行動裝置遭感染，該惡意 APP 不僅能取得手機型號、作業版本、系統及應用程式列表等資訊，還能竊取受害者的 APP 帳號、聯絡人資料及簡訊內容，並可遠端撥號、接收及寄送簡訊，洩漏的個人資料超過 100 萬筆，感染範圍擴及全球 55 個國家。

針對本類型發生原因，分析多因設備身分鑑別與授權不足，其中多因使用不安全的密碼或未做好適當的權限管理所致。

六、個人資料管理威脅持續存在

個人資料檔案一直是有心人士覬覦之目標，107 年政府機關出現若干個資外洩事件，分析駭客攻擊手法，仍以針對特定目標之電子郵件進行社交工程攻擊後，進而入侵政府機關電腦及竊取資料為常見案例外。另外，駭客透過入侵閒置無人管理之資訊系統，成功竊取個人資料之情形亦有之。

在攻防演練測試案例上，不安全的程式碼開發及同仁誤將個資置於公開網站亦為常見資料外洩原因。

伍、資安防護建議

針對本報告前述資安威脅，提供防護建議如下：

（一）針對 109 年即將到來之總統及立法委員選舉期間，各政府機關後續仍應加強防範假冒公務名義發送選舉相關之惡意電子郵件，以降低電腦中毒及機敏公務資料外洩之風險。

（二）為避免資通系統遭植入挖礦程式，政府機關仍應落實各項資安防護基本作業，包含確實修補系統弱點、阻擋惡意網域清單、定期執行瀏覽器以及相關套件安全性更新、加強使用者資通安全宣導等。

（三）針對政府委外供應鏈遭受攻擊之情形，機關應依據「資通安全管理法施行細則」第 4 條各款規定辦理，強化對委外廠商之資安要求及監督管理；另為降低國家資安風險，亦應依據「各機關對危害國家資通安全產品限制使用原則」規定辦理相關採購管理事宜，以及定期盤點資訊設備，下架之資通系統應依標準作業程序確實辦理下架作業。

（四）工業控制系統及 IoT 設備威脅持續升高，政府機關應將其納入機關資通資產盤點範圍，並加強辦理防護作為如下：

1. 新購或轉移資通訊設備應立即修改預設密碼，正式上線前，刪除預設帳號或更新密碼是基本防範之道。
2. 關閉不必要開啟之通訊埠，資訊設備相關應用程式與元件應建立最小權限存取控制原則。
3. 定期進行安全性軟韌更新或程式升級，並即時關注設備之漏洞發布提高警覺。
4. 除一般資訊設備之安全檢測外，路由器、網路攝影機、網路印表機及門禁系統等辦公室連網設備，都應納入檢測範圍。

（五）在降低個人資料外洩風險方面，唯有各機關落實各項資安防護工作實為根本之道。此外，初期設計即應融入資安(security by design)之觀念已逐漸被重視，因此，各機關在辦理大型資通系統建置時，即應導入安全程式開發週期(SSDLC)，提升軟體程式開發水準。

陸、結語

隨著人工智慧(Artificial Intelligence，簡稱 AI)應用、5G 結合物聯網與雲端服務等新興科技的崛起，未來之資安防護挑戰亦將更為嚴峻，駭客攻擊行為將朝精準化且善於規避偵測工具面向發展，其攻擊模式不僅多樣化，更可因應攻守情勢，彈性快速發展精細且精準之攻擊模式，國內公私部門皆應審慎以對，本院後續仍將依據資安法責成各政府機關落實各資安防護作為，並透過公私協力合作模式，促進資安威脅情資之共享，連結各界力量合作聯防，共同提升國家資安防護量能。

柒、附錄

[1] World Economic Forum (WEF), The Global Risks Report 2018, 13th Edition，來源連結：http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[2] 思科(Cisco) 2018 年網路安全報告，來源連結：https://www.cisco.com/c/dam/global/zh_tw/products/security/acr-report-2018/final_files_cisco_2018_acr_web_tw.pdf

[3] https://www.gao.gov/assets/700/694913.pdf

[4] 趨勢科技 2019 年資安預測報告，來源連結：https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019

[5] NIST Framework for Imporving Critical Infrastrucute Cybersecurity, 2018, Version 1.1，來源連結：https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[6] https://www.ithome.com.tw/news/126881

[7] https://nicst.ey.gov.tw/File/1C92657790845A40?A=C