109年第2季資通安全技術報告

Quarterly Technical Report

目　次

圖 目 次

摘要

「第 2 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關於資安風險的關注重點。

「第 2 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為國際機場網站遭駭客掛碼竊取使用者帳號密碼；另一起案例為針對能源產業之魚叉式網路釣魚(Spear Phishing)攻擊事件。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 64.38%) 類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」 (占 9.59%)與「設備問題」(占 5.94 %)為主要通報類型。

●2.資安專題分享

資安專題分享主題為 Microsoft Exchange 記憶體損毀漏洞，駭客利用 Exchange 伺服器漏洞(CVE-2020-0688)入侵，藉由此漏洞成功入侵後，可造成 Microsoft Exchange 記憶體損毀。此漏洞存在於開啟 Webmail 服務之 Exchange 伺服器，應儘速修補相關漏洞，並檢視是否有遭入侵之跡象。

●3.資安技術研析

資安技術研析主題為離地攻擊(Living off the Land, LotL)趨勢與研析，離地攻擊主要利用作業系統原生、非客製化之工具或命令、雲端服務搭配無檔案式記憶體操作(memory-only)進行攻擊。離地攻擊並非全新概念，但利用系統內建管理工具，配合外部雲端服務與記憶體操作之無檔案式操作，使離地攻擊成為近期常見之攻擊模式。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享 Microsoft Exchange 記憶體損毀漏洞，提醒機關相關風險之因應，並及早進行漏洞修補作業。此外，資安技術研析，概述離地攻擊趨勢與研析，並說明偵測與因應機制。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因與可能之衝擊與影響。109 年第 2 季(以下簡稱本季)探討系統不論是上線前或是進入維護週期時，皆有風險持續暴露或衍生之議題。另外，社交工程攻擊事件時有所聞，駭客社交工程手法加入業務真實情節或時事話題後展開攻擊，一旦被郵件防護系統或防毒軟體掃描無惡意程式，再加上使用者誤認為來自可信任的來源，則可成功達成駭侵目的。

本章節之事件與議題皆配合整理相關之資安防護重點，提供組織就相關資安風險或議題進行評估，並依循資安防護重點進行強化。

1.1 全球資安威脅現況

資通安全之關鍵環節是嚴謹的存取控制機制，若能在第一時間做好資安防護控管，則可大幅降低因駭侵所必須付出之代價。完善的存取控制機制，包含從資通系統開發時，確保遵循安全系統發展生命週期，時時注意資通系統漏洞之補強，以防堵對外公開系統遭掛碼，進而被竊取使用者憑證事件。

另外，須關注的資安威脅發展則來自於魚叉或目標鎖定的網路釣魚事件。相較於漫無目的地展開攻擊，魚叉或目標鎖定的網路釣魚攻擊事件有逐漸興起之勢。駭客除鎖定特定目標展開攻擊外，常用的手法仍為透過社交工程郵件做為入侵途徑，駭客為提高攻擊成功機會，更精進使用該領域特定之專業術語，並輔以真實事件，取得目標對象的信賴而開啟。

本季具指標性案例為國際機場網站遭駭客掛碼，竊取使用者帳號密碼；另一起案例為針對能源產業之魚叉式網路釣魚攻擊事件。

首先，探討案例為舊金山國際機場(San Francisco International Airport, SFO)網站遭駭客掛碼，竊取使用者帳號密碼。SFO 於 109 年 4 月 7 日發布資料

外洩公告(Notice of Data Breach)，證實 3 月時隸屬於 SFO 之 2 個網站(SFOConnect.com 與 SFOConstruction.com)皆遭駭客植入惡意程式碼，藉以竊取使用者帳號與密碼。

依據所公告內容，受攻擊之影響範圍涵蓋經由外部網路(非 SFO 機場內部網路)，使用 Windows 作業系統內建之 IE 瀏覽器存取受駭網站的使用者，以及經由內部網路使用非 SFO 維護設備存取受駭網站之使用者，主要目的為竊取使用者主機設備之帳號與密碼。

第 2 起案例為針對能源產業之魚叉式網路釣魚攻擊事件，資安業者 Bitdefender 研究人員發現 2 宗針對能源產業之魚叉式網路釣魚攻擊事件，駭客透過寄送精心製作之釣魚郵件予收件人，誘騙收件人點擊郵件附檔，以安裝 Agent Tesla 木馬程式。

第 1 宗魚叉式網路釣魚攻擊事件發生於 3 月 31 日，於一週內約 150 家分別位於馬來西亞、美國、伊朗及南非等國之石油與天然氣公司均遭受到同樣之釣魚攻擊。駭客假冒埃及知名石油暨加工工程承包商 Enppi 之名義寄送釣魚郵件，請收件人對名為「Rosetta Sharing Facilities Project」之計畫設備與材料進行投標。

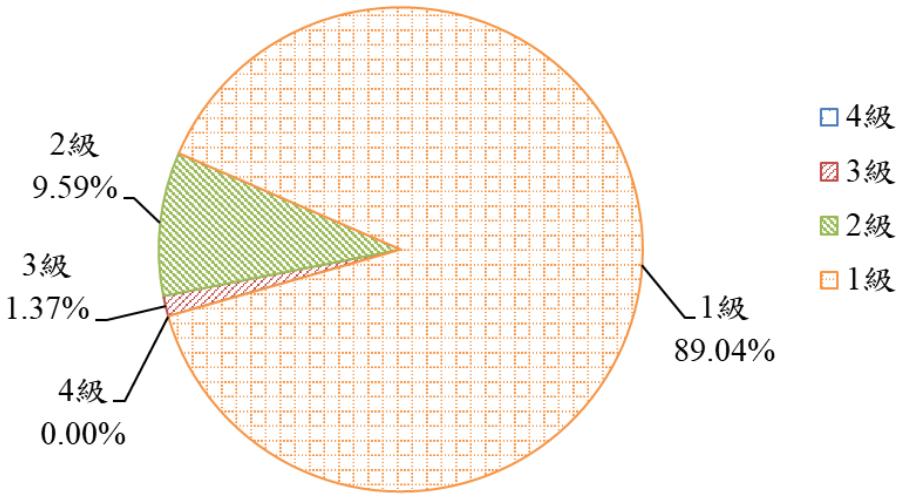
第 2 宗魚叉式網路釣魚攻擊事件發生於 4 月 12 日，於 2 天內有 18 家船務公司遭受同樣之釣魚攻擊，其中 15 家為菲律賓船務公司。駭客請收件人填寫一份石油郵輪 MarineTraffic 號之預估港口使用運費(Estimated Port Disbursement Account, EPDA)文件；該郵輪為印尼之真實船隻，於 4 月 12 日離開港口，並預計於 4 月 14 日抵達目的地。駭客透過加入業務真實情節或當下流行時事之話題，成功針對目標收件人進行魚叉式網路釣魚攻擊。

綜覽本季重大資安事件，發現在系統開發時需規劃採行安全系統發展生命週期，更應檢視相關系統維護之安全，特別是將重要系統委外開發或維護

時更應加強管理責任。同時，面對魚叉式網路釣魚攻擊，更應精進資安偵測與防護措施，並對機敏資料採取權限區隔或加密等機制。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 89.04%為大宗，2 級事件占 9.59%次之，3 級事件僅占 1.37%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

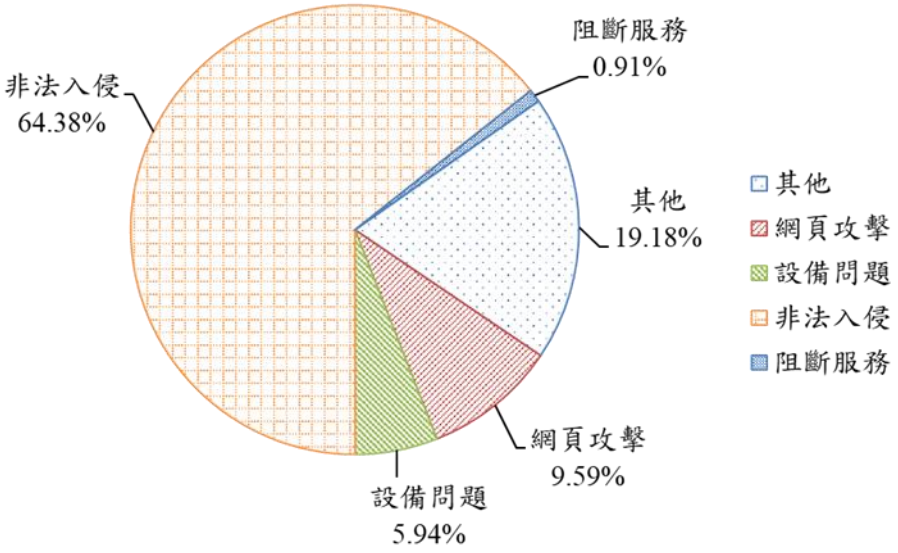


資料來源：本報告整理

圖1　109 年第 2 季通報事件影響等級比率圖

本季接獲之 3 級重要通報事件，為某機關因應新型冠狀病毒防疫作業，民眾進入須採取實名制登記，由委外廠商協助建立之 Google 表單因試算表權限設定錯誤，導致可公開檢索與編輯，內容因涉及民眾姓名、電話、近 14 天出國等個人資料，評估為個人資料外洩，故通報為 3 級重要事件。

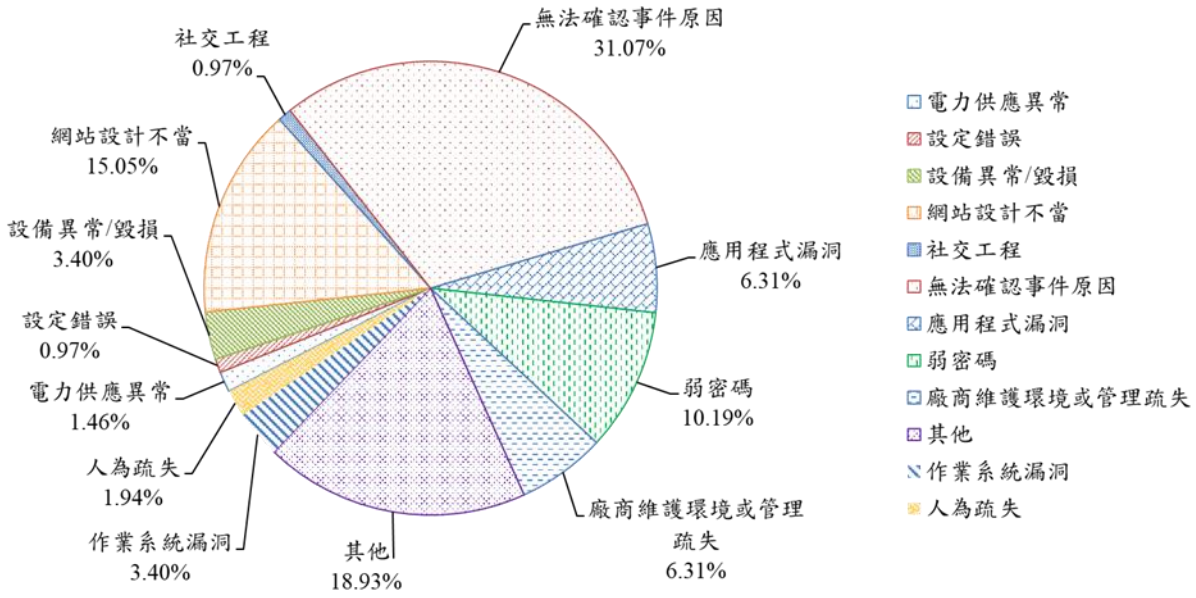
通報事件中發現駭客利用供應鏈進行攻擊活動，駭客利用廠商系統維護帳號入侵，再成功植入惡意程式。其他以非法入侵遭植入惡意程式或可疑連線居多，部分機關因網站存在漏洞或弱密碼，遭駭客利用後入侵植入後門程式，進而橫向擴散內部主機。整體事件比率，以「非法入侵」(占64.38%)類型為主，排除綜合類型「其他」外，「網頁攻擊」與「設備問題」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　109 年第 2 季通報類型比率圖

最後，分析通報事件發生原因，以無法確認事件原因(31.07%)、其他(18.93%)及網站設計不當(15.05%)位居前三名，其次分別為弱密碼(10.19%)、應用程式漏洞(6.31%)、廠商維護環境或管理疏失(6.31%)、作業系統漏洞(3.40%)、設備異常/毀損(3.40%)、人為疏失(1.94 %)、電力供應異常(1.46%)、社交工程(0.97%)及設定錯誤(0.97%)，詳見圖 3。本季一般事件發生原因以無法確認事件原因為主，占 31.07%，大部分為監視器設備受害，因設備受限無法存放日誌紀錄，無法調查遭入侵原因，故以「無法確認事件原因-無相關紀錄可供檢視」進行結案。



資料來源：本報告整理

圖3　109 年第 2 季通報事件發生原因比率圖

分析第 2 季通報事件發生原因，發現有機關接獲技服中心入侵事件警訊通知其內部主機遭入侵產生可疑連線，經調查發現可疑連線設備為個人電腦，依使用者瀏覽紀錄推測應為不當下載應用程式造成。該機關處置方式為將個人電腦重灌，並未再確認事件發生根因，亦未調查是否有內部擴散情況。相隔數天後該機關再次接獲技服中心入侵事件警訊，經查該受害設備與前次通報設備相同，因當時僅將設備重灌，未擴大進行事件調查而導致駭客於內部橫向擴散至其他設備，成功植入 VPN 工具並連線駭客中繼站。

1.3 資安防護重點

分析本季全球資安威脅現況，國際機場網站遭駭客掛碼，竊取使用者帳號密碼。公開服務網站一直以來是駭客首選目標，駭客藉由不斷偵測網頁漏洞，達到入侵之目的。因此對外網站除上線前之源碼、弱點檢測外，在正式維運後亦應定期安排檢測是否有新的系統漏洞。隨著魚叉式網路釣魚攻

擊事件的盛行，伴隨著駭客透過業務真實情節或當下流行時事之話題，成功針對目標收件人進行魚叉式網路釣魚攻擊，因此針對使用者規劃社交工程教育訓練，仍必須按步就班落實執行。

分析政府機關通報事件發現，資通安全事件處理仍有未臻完善處，未能遵循事件通報機制與標準程序完成事件處理，導致受害狀況再次發生。同時，發現駭客持續透過供應鏈展開攻擊，利用系統漏洞或廠商維護帳號，成功入侵開發/維護之資通系統。

綜整以上資安威脅現況，提供資安防護建議如下：

●魚叉式網路釣魚攻擊事件資安管理

– 建置網路釣魚信件偵測機制，精進惡意郵件分析與防堵。

– 電子郵件安全組態部署，同時定期檢視使用者相關設定之落實與正確性。

– 以事件案例宣導，強化使用者對社交工程辨識與因應之資安認知與意識。

●資通安全事件資安管理

– 遵循「資通安全事件通報及應變辦法」，建立內部通報及應變機制。

– 事件發生時應依程序進行損害控制與復原作業，並應持續進行資通安全事件之調查及處理，落實改善報告。

– 內部進行資通安全事件教育訓練與宣導，具體規劃與提出預防與矯正措施方案，避免事件再次發生。

●委外廠商資安管理

– 訂定服務水準協議，明確敘明工作項目之服務品質定義、權利義務歸

屬及預期目標與要求等。

– 定期檢視委外廠商之資通安全維護措施，規劃事件演練及通報應變機制。

– 設定維護廠商之存取權限，並強化日誌設定或網段切割，以避免造成橫向擴散，影響內部其他系統。

2. 資安專題分享_Microsoft Exchange 記憶體損毀漏洞

技服中心陸續接獲機關通報郵件伺服器遭入侵事件，經了解受害情況，推測為駭客利用 Exchange 伺服器漏洞(CVE-2020-0688)入侵。駭客藉由此漏洞成功入侵後，可造成 Microsoft Exchange 記憶體損毀。

當資通系統存在相關弱點被揭露後，首先可以發現網路上會出現大量掃描偵測是否使用相關軟硬體。因此，當機關獲知所使用系統存在相關風險時，應於完成業務持續運作相關衝擊評估後，儘快進行漏洞修補作業。

另外，因漏洞存在於開啟 Webmail 服務之 Exchange 伺服器，若機關未開啟 Webmail 服務，則不存在此漏洞風險。意謂著管理者在資通系統上線前，應全面檢視是否有預設開啟且不需使用之服務，以降低可能之風險。

為協助資安人員及早加強防護作為，以下針對 CVE-2020-0688 漏洞進行研析，以掌握漏洞影響範圍與相關防護措施。

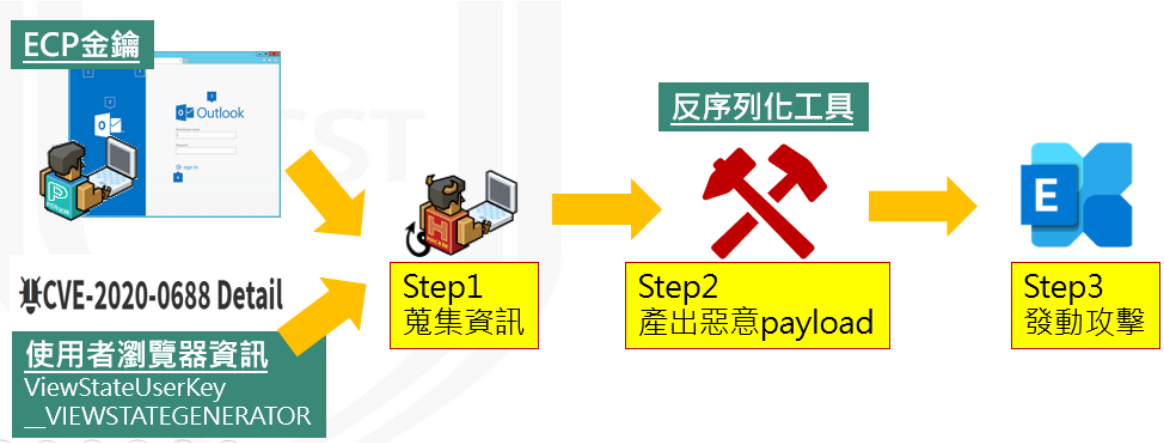
2.1 CVE-2020-0688 漏洞說明

CVE-2020-0688 漏洞允許攻擊者遠端執行任意程式碼，影響 Exchange 伺服器 2010、2013、2016、2019 等版本，微軟公司將此漏洞之嚴重程度列為「重要」等級。NIST 將 CVE-2020-0688 評分為 8.8(CVSS Version 3.X)與 9.0(CVSS Version 2.0)。此漏洞肇因在於 Exchange 伺服器並未建立唯一獨立金鑰，每台 Exchange 伺服器安裝時皆會使用同一金鑰，使得攻擊者可透過授權使用者取得金鑰，利用傳遞特製封包到 Exchange 伺服器，導致記憶體毀損。

Exchange 伺服器安裝過程中，Exchange Control Panel(ECP)元件會建立相同的 validationKey 與 decryptionKey，並寫入 web.config 檔案，做為使用者端瀏覽器 ViewState 控制項執行狀況的對應參照。ViewState 則用來儲存網

頁上伺服器控制項資訊，保存使用者端與伺服器端來回存取(Postback)間之網頁與控制項值，以進行狀態管理，該控制項暫存於用戶端瀏覽器中。

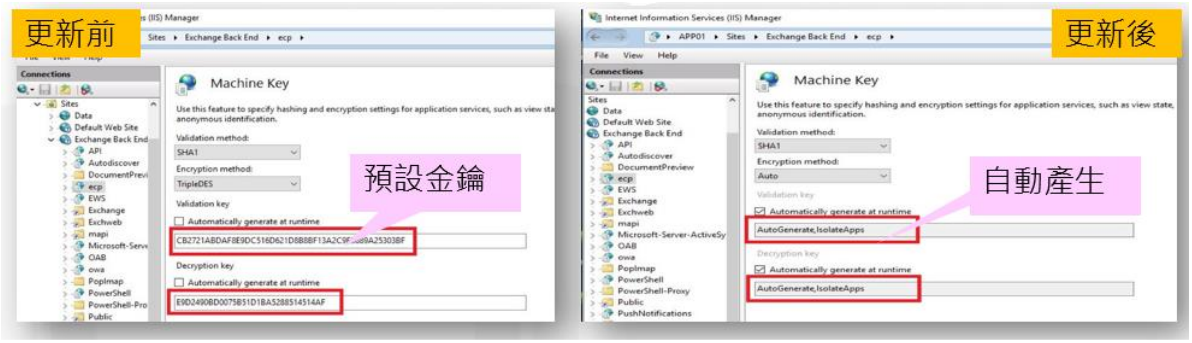
此漏洞需滿足 2 項條件才可觸發利用，並透過反序列化工具(如 YSoSerial.net 等)進行攻擊活動。首先，要取得 Exchange 伺服器使用相同的 validationKey，再來則須取得使用者瀏覽器資訊，取得此資訊並不需要為管理者權限，詳見圖 4。



資料來源：本報告整理

圖4　利用共同金鑰展開攻擊

微軟公司於 2 月 11 日釋出更新程式，調整 ECP 金鑰為執行時「自動產生」，每次金鑰不再相同，詳見圖 5。

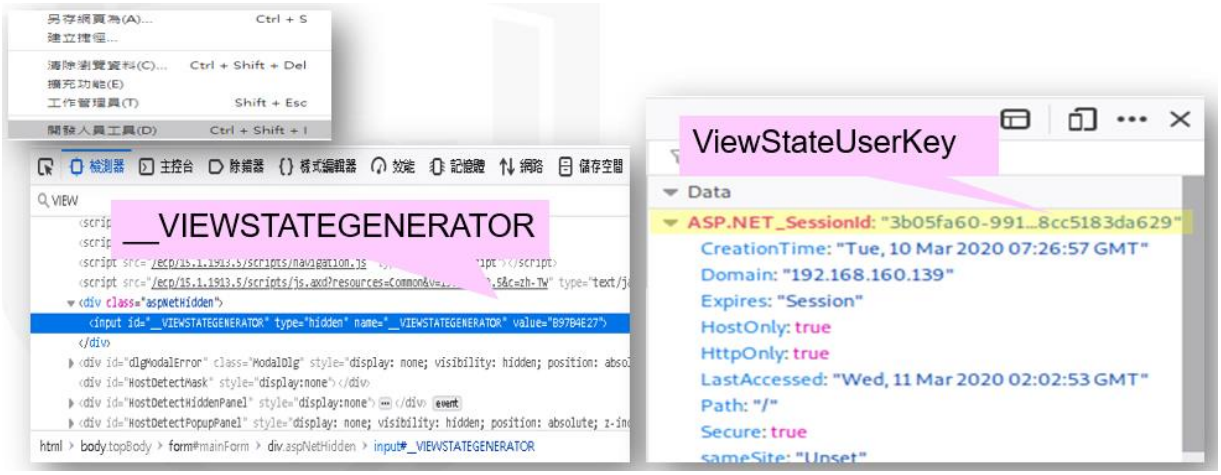


資料來源：本報告整理

圖5　更新後自動產生金鑰

2.2 漏洞利用與應對方式

攻擊者首先取得一組使用者帳號密碼登入系統，透過瀏覽器開發人員工具，取得 ViewStateUserKey 與__VIEWSTATEGENERATOR 值，ViewStateUserKey 存於 ASP.NET_SessionId 欄位中，詳見圖 6。



資料來源：本報告整理

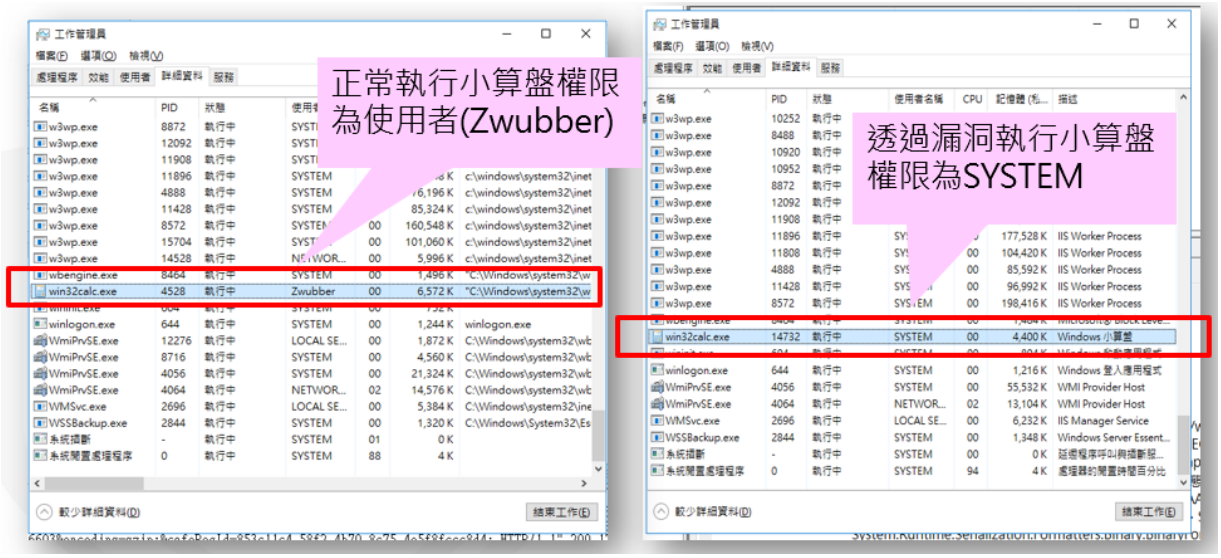
圖6　透過帳密獲取 ViewStateUserKey

透過反序列化工具 YSoSerial.net，整合已蒐集資訊，以下將以啟動小算盤為例，產生惡意封包內容，詳見圖 7。

資料來源：本報告整理

圖7　惡意封包內容

接續攻擊者可透過 WEB 或 CMD 方式，於存在漏洞頁面(如 /ecp/default.aspx 等)塞入惡意封包，進行攻擊活動。由於 ECP 是以 SYSTEM 權限執行，因此受害 Exchange 伺服器可發現以 SYSTEM 權限產生在背景執行的小算盤，詳見圖 8。



資料來源：本報告整理

圖8　以 SYSTEM 權限產生在背景執行小算盤

利用漏洞頁面進行攻擊，將使 Exchange 伺服器產生錯誤，因此可透過 Event Log 發現攻擊軌跡。同時在 IIS log 也可發現攻擊軌跡，因攻擊過程中需利用__VIEWSTATE 參數，在攻擊目標 URL 進行 POST/GET 請求，然而正常行為中__VIEWSTATE 不應出現在 GET 請求中。最後一個攻擊軌跡調查則為透過分析後發現，__VIEWSTATE 參數內容使用 Base64 編碼，可嘗試解碼還原駭客攻擊行為，詳見圖 9。

資料來源：本報告整理

圖9　解碼還原駭客攻擊行為

政府機關事件案例中，發現有 Exchange 伺服器遭新增異常檔案，駭客獲取合法登入之使用者帳號密碼後，利用 CVE-2020-0688 漏洞植入惡意程式。另有案例為 Exchange 伺服器遭植入惡意程式後，連線至駭客中繼站，進一步檢視 IIS Log 紀錄，發現駭客攻擊活動軌跡，研判駭客利用 CVE-2020-0688 漏洞植入 Webshell，並透過該 Webshell 陸續上傳惡意程式。

相關應變與處置首要作為是先行檢視若有開啟 Webmail 服務之伺服器，應儘速進行更新。再者，此漏洞為 2 階段式攻擊，攻擊者須取得授權使用者帳號密碼，方可透過漏洞進行攻擊。針對弱密碼或有其缺陷之資通系統，應先行變更帳號密碼，並確認該使用者之資通設備是否受害。最後，可解譯駭客使用之攻擊指令，進而採取對應之防護修補措施，如透過駭客攻擊活動軌跡，分析遭利用之使用者與行為，加強資安防護作為與教育訓練。

3.資安技術研析_離地攻擊趨勢與研析

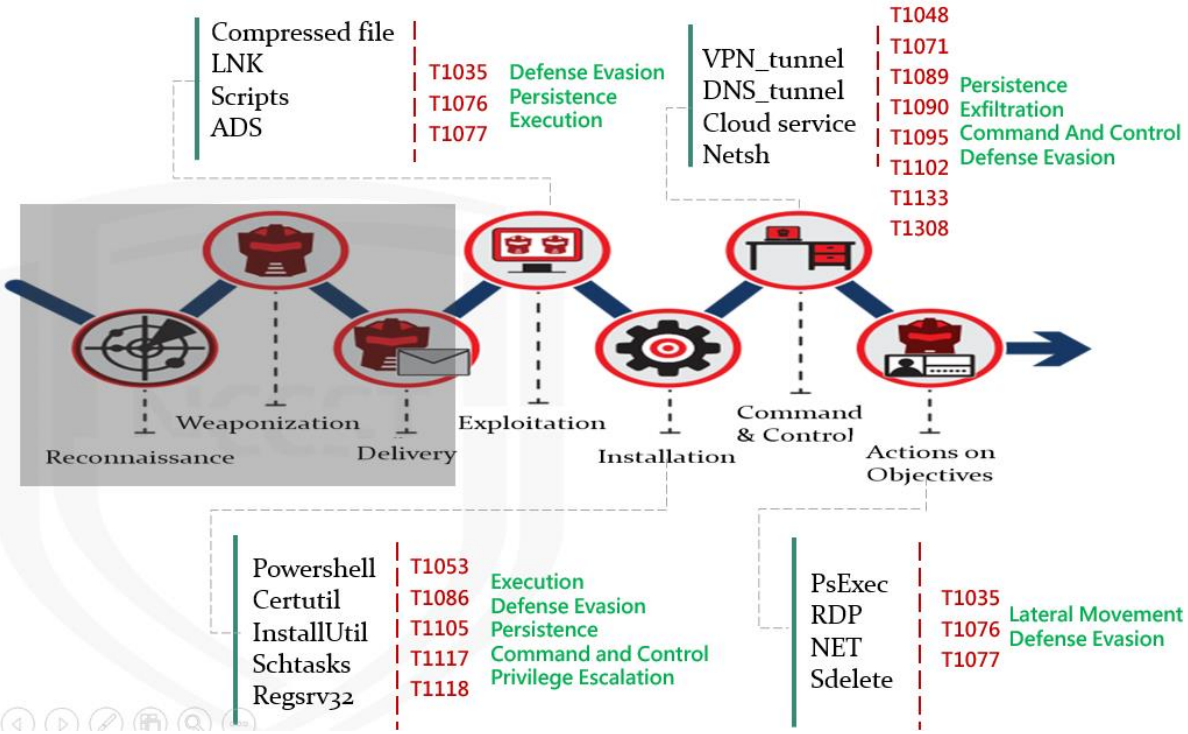
本季所探討的資安技術研析為離地攻擊趨勢與研析，技服中心觀察近期政府骨幹攻擊活動與政府機關資安事件發現，已知的特定組織型駭侵之客製化樣本活動有逐漸減少之現象，而離地攻擊手法使用之頻率，卻有明顯增加之趨勢。

離地攻擊並非全新概念，但利用系統內建管理工具，配合外部雲端服務與記憶體操作之無檔案式操作，使離地攻擊成為近期常見之攻擊模式。

3.1 離地攻擊手法分析

離地攻擊主要利用作業系統原生、非客製化之工具或命令、雲端服務，搭配無檔案式記憶體操作進行攻擊。主要攻擊優勢在於不需要多餘成本準備客製化攻擊樣本，同時規避外部偵測與端點防護機制，完整隱藏實際攻擊之發動者(threat actor)，大幅增加鑑識調查困難度。

以下彙整離地攻擊中常見被利用之工具與手法，以及對照其在網路攻擊鏈(Cyber Kill Chain)之階段，相關關聯彙整與對照詳見圖 10。



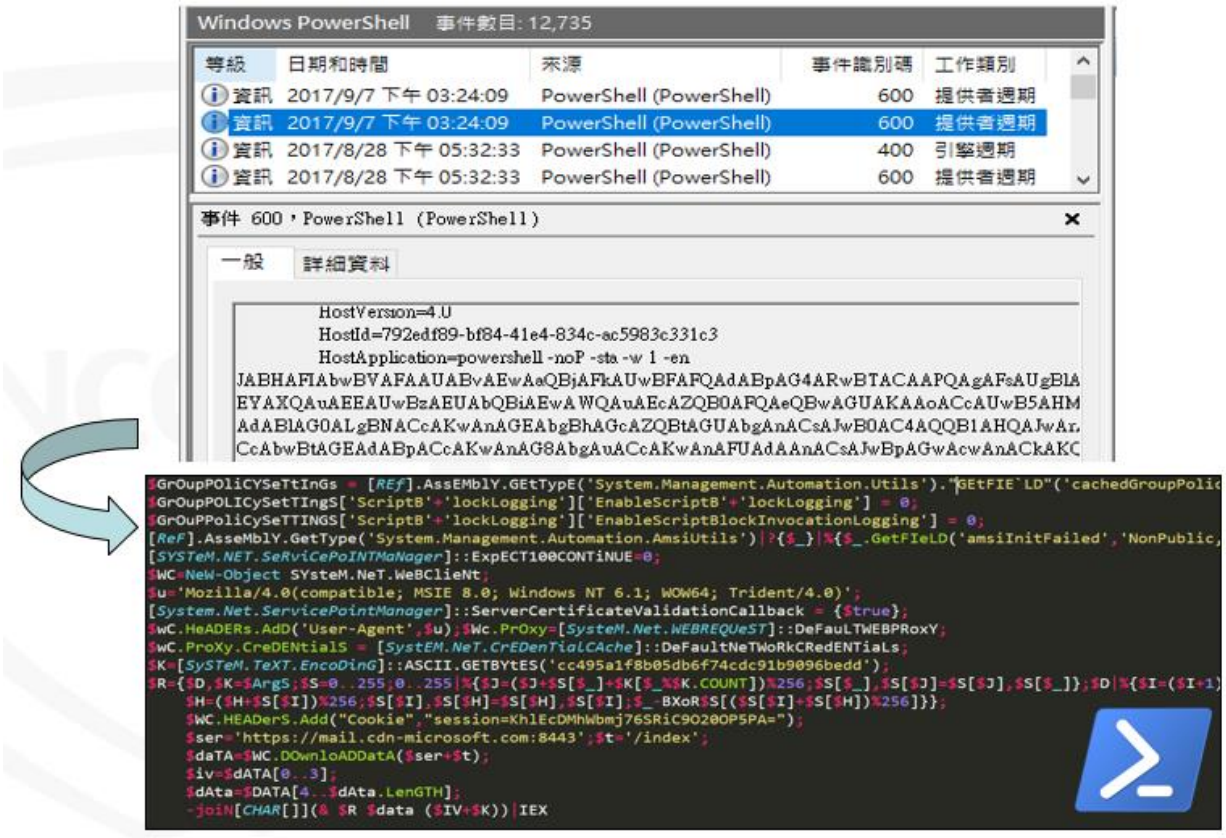
資料來源：本報告整理

圖10 離地攻擊中常見工具與手法對照網路攻擊鏈

以下透過相關範例，說明離地攻擊所使用的工具與手法。

●Powershell

離地攻擊常利用系統管理工具 Powershell 對主機進行高權限操作，常見被用於遠端下載及將惡意指令載入記憶體中執行。此攻擊手法可對應到網路攻擊鏈之安裝(installation)、命令與控制(Command and Control)及目標鎖定攻擊(Action on objectives)階段。如利用 Powershell 至 Github 下載惡意程式腳本(mimikatz)後，再利用 Powershell 執行編碼後之惡意程式，詳見圖 11。



資料來源：本報告整理

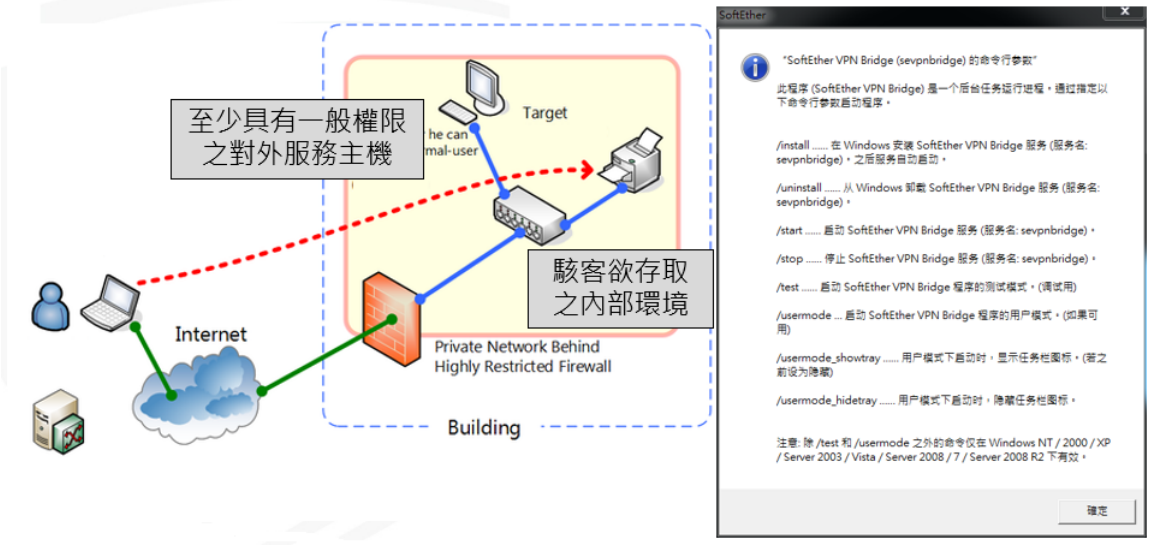
圖11 執行編碼後之惡意程式

●VPN Tunnel

VPN Tunnel 目的為對外建立 VPN 通道，使駭客控制端與受害機關端形成同一內網利於橫向移動，規避防護與偵測機制，此攻擊手法可對應到網路攻擊鏈之命令與控制階段。近期發現攻擊者常用 SoftEther VPN 建立 VPN 通道，該工具包含 3 個部分，包含主程式 (vpnbridge.exe/vpnserver.exe)、連線設定檔(vpn_bridge.config/vpn_server.config)及 VPN 驅動(hamcore.se2)。建立方法為藉由 VPN 伺服器建立多個虛擬集線器，讓遠端 Client 或 Bridge 來連接，而 VPN Bridge 可用來建立一個虛擬集線器，將 Local LAN 橋接到遠端伺服器。

攻擊者通常會先入侵機關對外服務網站，接著在內部尋找可利用主機，

找到後安裝 VPN 工具，讓攻擊者可以隨時自外部進行存取並橫向移動，詳見圖 12。



資料來源：本報告整理

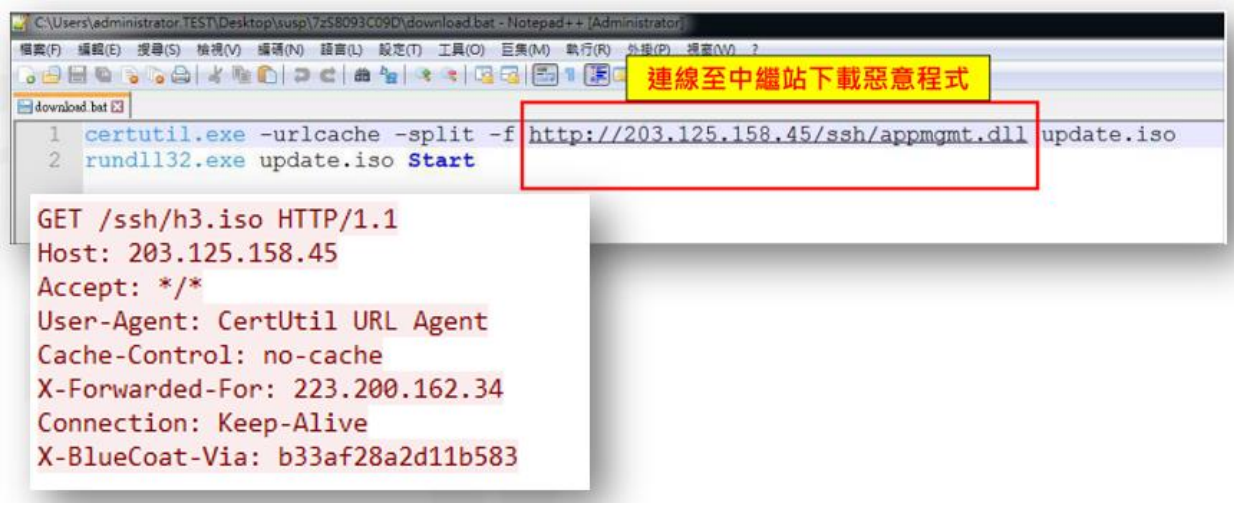
圖12 利用 SoftEther VPN 建立 VPN 通道

運用該工具於 VPN Tunnel 上，測試發現各家防毒軟體偵測結果，均判斷為正常程式，顯見偵測之難度。

●CertUtil

CertUtil 系統管理工具主要用於憑證操作，以顯示憑證授權單位(CA)設定資訊、設定憑證服務等。在相關駭侵案例中，常被用於遠端下載惡意程式，此攻擊手法可對應到網路攻擊鏈之安裝階段。

駭客利用該工具自遠端中繼站下載惡意程式後執行，詳見圖 13。



資料來源：本報告整理

圖13 遠線至中斷站下載惡意程式

因 CertUtil 工具提供編碼與解碼功能，駭客可藉此規避偵測機制，致資安防護人員無法在入侵第一時間發現。

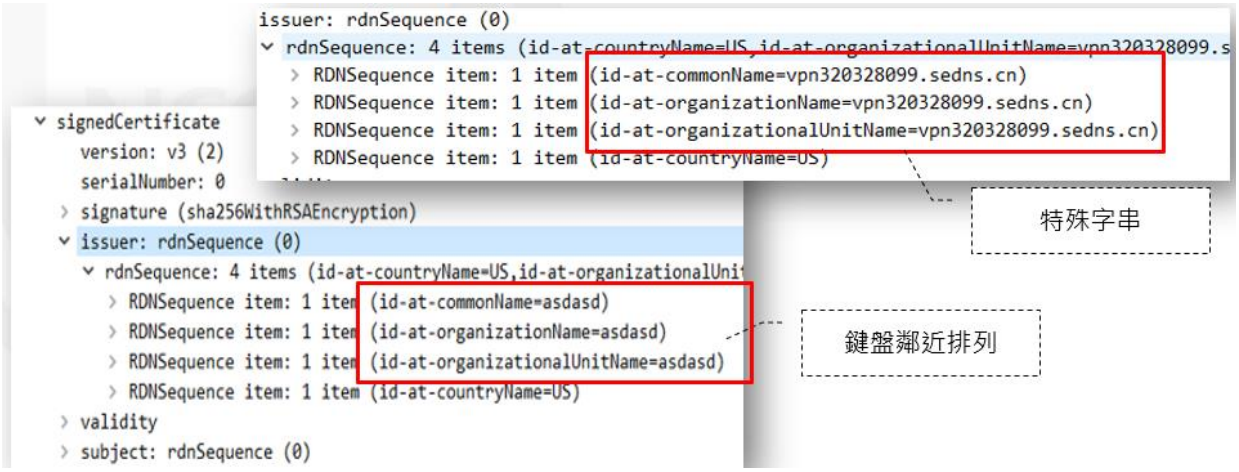
3.2 偵測與因應機制

離地攻擊防禦首要是避免惡意或未知的執行檔運作，若未能成功阻擋，則應限制或透過隔離這些執行檔持續運作所造成的損害。這些執行檔通常出現在網路攻擊鏈的末端，因此如何提升資安防護作為或即時偵測異常活動，以避免攻擊來到最後階段，是管理者必須思考之課題。

離地攻擊目標為進入受害環境後，利用內建工具、系統指令，規避端點與外部監控防護機制。尤其駭客更強化其操控之隱蔽性，更利於內部進行攻擊擴散。而根本防護之道首重一般入侵防護，如電子郵件防護政策，防範社交工程郵件入侵、加強對外服務網站防護及資通系統與軟體即時更新，以阻絕惡意程式進入目標環境。

另外，可藉由分析流量以偵測駭客所使用之特殊工具，嘗試研析其攻擊模式，如比對從事件處理所獲樣本與骨幹流量，VPN 於加密前會利用三向交

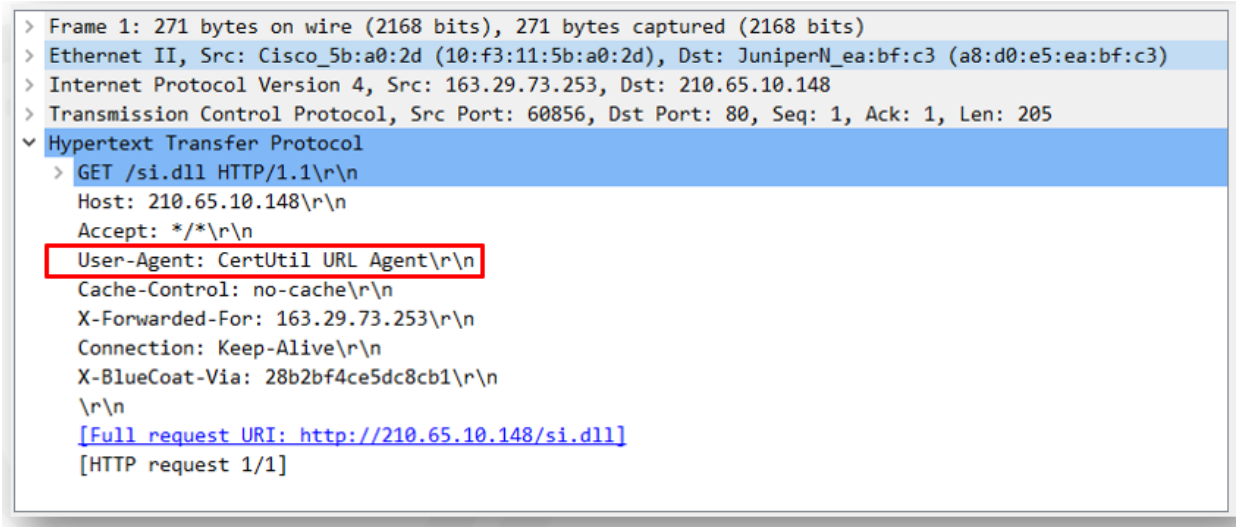
握溝通加密方式與憑證資訊，發現駭客利用之工具 SoftEther VPN 具有自產憑證功能，內容為自行填寫之憑證資訊，詳見圖 14。



資料來源：本報告整理

圖14 SoftEther VPN 自產憑證

另外，其他異常網路流量分析包含偵測 CertUtil，駭客利用此工具下載惡意程式，其網路流量會有特定網路特徵，詳見圖 15。



資料來源：本報告整理

圖15 CertUtil 異常網路特徵

離地攻擊類型近期呈現大幅成長，推測整體攻擊戰術有所變化，將持續觀

察惡意行為，包含透過系統內建工具下載/啟動惡意程式、以 VPN 或 DNS 通道建立控制連線及配合無檔案形式將惡意行為載入記憶體執行等攻擊方式。配合初期之入侵預防，儘可能阻絕攻擊者進入目標環境為優先，再進行異常活動偵測機制，如大量 VPN 連線、異常 DNS 查詢等，則可降低其成功入侵之可能性。

4. 結論

本季具指標性案例為透過國際機場網站遭駭客掛碼竊取使用者帳號密碼，對使用者來說使用公開網路服務更應提高資安警覺，對於資通系統管理者則應定期檢測網站之安全；另一起案例為針對能源產業之魚叉式網路釣魚攻擊事件，此類攻擊事件日益增多，應精進資安防護方案，尤其是加強電子郵件與資料存取之監督管理，同時持續以事件案例做為經驗學習與分享，教育使用者如何更精準辨識來自於魚叉式網路釣魚之社交工程攻擊。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 64.38%)類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」與「設備問題」為主要通報類型。針對本季全球與政府所面臨的主要資安威脅，本報告就「魚叉式網路釣魚攻擊事件資安管理」、「資通安全事件資安管理」及「委外廠商資安管理」，提出資安防護建議。

資安專題分享 Microsoft Exchange 記憶體損毀漏洞事件，技服中心陸續接獲機關通報郵件伺服器遭入侵事件，分析駭客利用 Exchange 伺服器漏洞(CVE-2020-0688)入侵，進而造成 Microsoft Exchange 記憶體損毀，應儘速進行漏洞修補，並檢視是否有相關遭駭軌跡。若已遭駭，則須透過分析駭客攻擊活動軌跡，辨識遭利用之使用者。除要求使用者立即變更帳號密碼外，亦應確認使用者資通設備受害狀況，並解譯駭客使用之攻擊指令，進而採取對應之防護修補措施。

另外，資安技術研析主題為離地攻擊趨勢與研析，觀察近期政府骨幹攻擊活動與政府機關資安事件發現，離地攻擊手法使用之頻率有明顯增加之趨勢。離地攻擊利用系統內建管理工具，配合外部雲端服務與記憶體操作之無檔案式操作。離地攻擊主要攻擊優勢在於不需要多餘成本準備客製化攻擊樣本，同時規避外部偵測與端點防護機制，增加鑑識調查困難度。透過分析離地攻擊手法，持續監控惡意行為，期能降低成功入侵之可能性。

資安相關活動

本季行政院資通安全處辦理之資安相關活動，說明如下：

◆ N-ISAC 定期會議

本次 N-ISAC 會議之專題分享主題為勒索軟體之防護策略與方案，邀請趨勢科技、微軟、安碁、調查局、經濟部針對不同防護面向進行說明，包含勒索軟體之演變與防護措施、透過中油與近期案件說明勒索軟體入侵方式與防護措施，以及從領域管理層面、SOC 監控層面等，如何進行強化與精進資安防護。

勒索軟體的散播途徑由惡意郵件、網頁掛馬及系統漏洞到新形態手法駭客購買廣告惡意誘騙，從之前漫無目的地攻擊，逐漸發現有更多案例為目標式勒索攻擊。以國內案例分析，發現能源與科技公司為遭鎖定的目標攻擊對象。重點防護機制分享包含檢視網路防護機制，檢視現有對外網路服務是否存在漏洞與破口、VPN 有無異常登入或異常網路流量、觀察 AD 伺服器群組原則是否遭異動或工作排程異常遭新增，同時加強監控網域之特權帳號，妥善建立備份機制，並離線保存。