111年第4季資通安全技術報告

Quarterly Technical Report

國家資通安全研究院

National Institute of Cyber Security

目　次

圖 目 次

表 目 次

摘要

「第 4 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，提供政府機關需關注之資安風險重點。

「第 4 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 Microsoft IIS Web 伺服器之日誌遭駭客運用於操控惡意程式；另一起案例為美國某家媒體公司因遭駭客入侵，引發後續供應鏈攻擊危機。

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 54.76%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 14.29%)與「網頁攻擊」(占 8.33%)為主要通報類型。

●2.資安專題分享

資安專題分享主題為 SSL VPN 安全部署，遠端連線安全所衍生之各項資安議題，政府機關應有漏洞偵測與揭露相關程序，並建立安全漏洞訊息處理機制，於接獲相關設備之漏洞警訊後，立即評估對業務之衝擊分析，規劃修補之優先順序。

●3.資安技術研析

資安技術研析主題為 AD 攻擊手法研析與 CVE 弱點驗證實作，藉由分析 AD 攻擊流程，了解入侵者如何進行本地權限提升與內部橫向移動，最終取得 AD 主機控制權。透過弱點驗證實作，得知駭客入侵步驟，並說明其弱點修補方式，以及建議管理者安全之組態設定與管理措施。

●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 SSL VPN 安全部署，提供 SSL VPN 部署常見錯誤樣態，除設備應部署於防火牆內部專屬區域外，設備管理介面與 SSL VPN 使用者亦應獨立部署於不同區域。此外，資安技術研析分析為 AD 攻擊手法研析與 CVE 弱點驗證實作，透過實作了解 AD 之常見攻擊手法與步驟，分析其入侵路徑，並提供弱點修補建議。

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及可能之衝擊與影響。111 年第 4 季(以下簡稱本季)探討社群媒體所衍生之相關資安議題與討論新興駭客技術攻擊所造成之可能衝擊與後果。

本章節之事件與議題皆配合整理相關之資安防護重點，提供政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

本季應特別關注的是 ISO 27001：2022 新版推出，在間隔 8 年之後，新版因應新興科技趨勢與著眼不同策略面向，更新與闡釋資訊安全管理制度之重點。新版標準分別從組織、人員、實體環境及技術等 4 大面向控制項，揭露資通安全除從原有管理與技術控制項外，亦應針對現有整備度不足與因應新興網路攻擊手法與型態，新增組態管理、網站過濾、程式碼安全及活動監控等強化措施。

全球資安威脅聚焦在新興攻擊手法之興起與複雜度持續提升，攻擊來源超越原有資通系統監管範圍與活動時，管理者籌劃處置與因應之道。面對來自供應鏈可能之威脅時，如何即時偵測或甚至於能在第一時間阻斷攻擊，可透過威脅情資之分享與主動式防禦機制成功遏阻。

本季具指標性案例為 Microsoft IIS Web 伺服器之日誌，遭駭客運用於操控惡意程式；另一起案例為美國某家媒體公司因遭駭客入侵，引發後續供應鏈攻擊危機。

首先，探討案例為Microsoft IIS Web 伺服器之日誌遭駭客運用於操控惡意軟體。資安廠商賽門鐵克揭露駭客組織 Cranefly(或稱 UNC3524)，藉著透過 Microsoft Internet Information Services (IIS) Web 伺服器日誌，達到控制

受感染設備上惡意程式之目的。Microsoft IIS 主要用途為建立網站與網頁應用程式之網頁伺服器，當使用者存取網頁時，Microsoft IIS 會將存取紀錄儲存至日誌檔中，日誌檔一般用於分析資料與故障排除。賽門鐵克揭露駭客組織正利用 IIS 日誌，於受駭電腦上安裝後門程式藉以發送命令。又因 Web 伺服器日誌單純用於儲存來自全球各地任何使用者之請求，因此管理者不會特別使用安全監控軟體監看其活動，而駭客就藉以利用儲存惡意指令，並隱藏其蹤跡。

研究人員並發現駭客組織 Cranefly 植入木馬程式「Trojan.Geppei」後，會自動安裝新興惡意軟體「Trojan.Danfuan」，利用此途徑則可直接從 IIS 日誌中讀取命令且蒐集資訊，而駭客藉由從 IIS 日誌尋找特定之字串，如 Wrde、Exco 及 Cllo 等，可再利用安裝其他惡意軟體、執行命令或停用 IIS 日誌記錄。目前所知，Cranefly 使用此種隱蔽技術於受感染之伺服器上潛藏，並蒐集情資。而因為此種新穎攻擊手法亦可透過 Proxy 代理伺服器、虛擬私人網路(VPN)或洋蔥路由器 Tor(The Onion Router)等各種方式向受駭伺服器傳送命令，更加深追蹤其蹤跡之難度。

第 2 起案例為美國某家媒體公司因遭駭客入侵，引發後續供應鏈攻擊危機。資安廠商 Proofpoint 觀察到該媒體公司主要提供影音內容與廣告予其他媒體新聞網站，提供方式是透過 JavaScript 指令碼。駭客藉由竄改此 JavaScript 之基礎程式碼(Codebase)，進而部署惡意程式 SocGholish，偽冒假更新(FakeUpdates)至逾 250 家新聞網站，因此引發一波供應鏈供擊之風波。

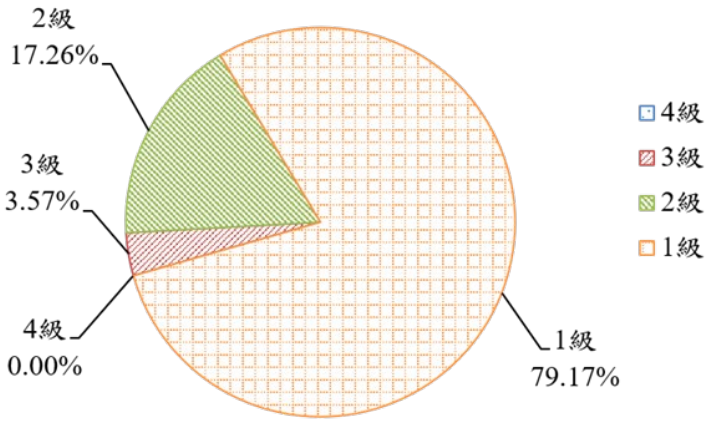
此次事件經 Proofpoint 追蹤後，顯示為俄羅斯駭客組織 TA569 利用新聞網站散布惡意軟體 SocGholish，導致受駭者遭植入勒索軟體等惡意軟體。且受駭網站以瀏覽器更新，如 Chrome.Updater.zip、Firefox.Update. zip、Opera.Update.zip 之名義，誘騙使用者下載內含鍵盤側錄工具(Keylogger)等

惡意軟體之壓縮檔案。同時 Proofpoint 觀察到受駭者成功修復後數日後又再次遭植入相同之惡意軟體，除使用者應加強資安意識外，亦表示清除惡意程式需竭盡系統管理者所能，並將事件於內部進行經驗學習案例分享，方能避免事件再次重演。FakeUpdates 通常採取保守入侵活動，不會貿然一次性地對大量目標對象釋出假更新，策略為對其潛在目標進行窺探與篩選，根據使用者之瀏覽器，跳出 Firefox、Chrome 或 Flash 等更新訊息，因此使用者通常無法於第一時間警覺發現。

綜覽本季全球資安威脅與資安事件，新式攻擊手法讓資通系統管理者應接不暇，又加上匿跡式入侵策略，致組織無法即時偵測，因此建立偵測規則，並適時更新以識別惡意活動，同時將供應鏈納入事件通報範圍，從內部防微杜漸，更能避免衝擊擴大至外部利害相關者。

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 個面向所造成之衝擊，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 79.17%為大宗，2 級事件占 17.26%次之，3 級事件僅占 3.57%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

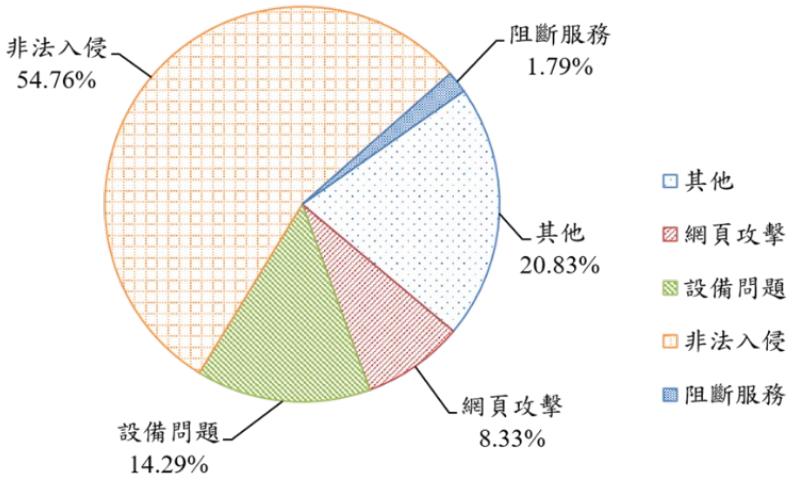


資料來源：本報告整理

圖1　111 年第 4 季通報事件影響等級比率圖

本季接獲之重要通報事件，有某機關委外營運之平台疑似個資外洩與駭客藉由廠商遠端維護管道植入惡意程式等事件，遠端存取控制機制應依「原則禁止、例外允許」方式辦理，若需外部遠端維護，應限制存取權限與強化監控措施，降低遭外部入侵風險。

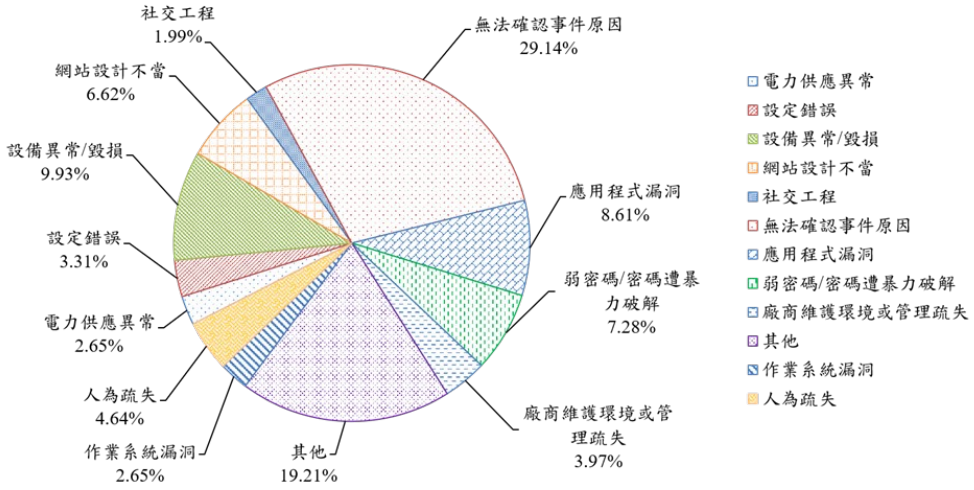
整體通報事件類型，以「非法入侵」(占 54.76%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　111 年第 4 季通報類型比率圖

非法入侵通報事件中，持續追蹤駭客利用紅隊演練工具 Cobalt Strike 與 Brute Ratel C4(BRC4)攻擊事件之樣態，近期發現駭客透過 Cobalt Stike 產製超過 5 種類型之惡意程式進行非法入侵。分析通報事件發生原因，以無法確認事件原因(29.14%)與其他(19.21%)為主，其次分別為設備異常/毀損(9.93%)、應用程式漏洞(8.61%)、弱密碼/密碼遭暴力破解(7.28 %)、網站設計不當(6.62%)、人為疏失(4.64%)、廠商維護環境或管理疏失(3.97%)、設定錯誤(3.31%)、電力供應異常(2.65%)、作業系統漏洞(2.65%)及社交工程(1.99%)，詳見圖 3。本季無法確認事件原因與其他之比例幾近五成，主要為無相關紀錄可供檢視與事件調查後仍無法確認原因所造成之結果，經進一步分析發現部分監視器設備出現異常連線，惟因監視器設備資源有限，未保存相關紀錄，導致無法確認事件發生原因。監控設備除要求預設密碼變更與存取權限控管外，採購相關設備時應要求具備日誌與警示之功能，方能記錄與回報異常之登入或連線行為，達到預警通報與追蹤之目的。



資料來源：本報告整理

圖3　111 年第 4 季資安事件發生原因比例圖

分析第 4 季通報類型與通報事件發生原因，設備問題所造成之異常或毀損為排名第 3 位之通報事件。經偵測發現多個機關資訊設備下載疑似殭屍網路(Botnet)相關惡意程式，入侵原因為網站或路由器存在漏洞，因而遭利用被植入惡意程式。而因其他設備異常或毀損情況則有組態設定錯誤、資料庫指令誤用導致資料庫系統異常、網路交換器管理模組、資料庫主機及網路交換器等硬體故障、負載平衡設備因磁碟區容量幾近滿載未清理致運作異常等不同狀況。硬體設備之基礎架構、組態設定、維運及容量管理之要求，從採購初始、上線、日常維運至中長期容量管理，皆應採取預設安全(Secure by Default)原則，從根本上解決安全問題。

1.3 資安防護重點

分析本季全球資安威脅現況，駭客使用 IIS 日誌檔於受駭電腦上安裝後門程式藉以發送命令，利用管理者日常不會特別監管其活動，而達成其操縱目的。而駭客就利用此機會，藉以儲存惡意指令，又可隱藏其蹤跡。另一威脅現況發現供應鏈攻擊危機仍高居不下，同時引發另一個議題為當不幸遭駭客入侵後，如何確認已無相關弱點或惡意程式存在，從經驗中學習如

何應處與避免再次被類似情況攻擊，除提升人員資安意識外，亦應謹慎檢視所有組態之安全設定。

國內部分偵測發現紅隊演練工具遭駭客運用於各式攻擊行動，駭客利用紅隊演練工具 Cobalt Strike 與 BRC4 產製惡意程式進行入侵攻擊，其中 BRC4 因具有規避現有防毒產品偵測之特性，使駭客攻擊行動更難被發現與追蹤。演練工具原為偵測資安弱點，及早因應以減緩風險，卻遭駭客濫用，故應研析駭客攻擊鏈中公開工具遭濫用情形，以利強化資安防護。

綜整以上資安威脅現況，提供資安防護建議如下：

●新興攻擊趨勢與手法之資安管理

– 針對新興科技如 AI、元宇宙及未來運算等議題，持續觀注並研提防禦建議。

– 建立威脅情資分類，如策略性(Strategic Threat Intelligence)、戰術上(Tactical Threat Intelligence)及操作性(Operational Threat Intelligence)，俾利清楚掌握資安情勢，訂定防禦政策及評估風險優先回應順序。

– 分析駭客族群之產業生態鏈(Ecosystem)，了解其相關供應鏈與鎖定弱點，同時將入侵威脅指標(Indicator of Compromise, IOC)部署於資安監控防護機制，分析可能威脅。

●設備鑑別與可靠性之資安管理

– 檢視設備安全架構與審視整體供應鏈，從硬體安全架構基礎解決根因議題，阻擋設備受到外部駭侵與毀損。

– 建立並執行基於軟體憑證或信賴平台模組(Trusted Platform Module, TPM)之公開金鑰密碼系統鑑別協議，確認使用者端點設備受到保護與管理。

– 建立監控設備健康管理機制，定期分析與監控設備日誌，評估設備與其他元件之健康狀態，包含作業系統、防毒、應用程式等更新與組態合規信賴程度，訂定維護或汰換時機。

2. 資安專題分享_ SSL VPN 安全部署

COVID-19 疫情在全球已接近尾聲，因應疫情發展漸趨成熟之遠距工作模式成為常態工作模式之一，遠端連線需求亦持續增加，遠端連線安全所衍生之各項資安議題除應逐一檢視，遠端連線架構與部署安全性更應在開放連線之前妥善規劃。

VPN 遠端連線之相關資安事件，早期即有有心人士刻意蒐集未修補漏洞之 SSL VPN IP 位址於暗網販售，藉以供買家利用某特定廠牌設備之漏洞輕易入侵目標對象。時至今日，駭客仍持續挖掘 VPN 設備之最新漏洞，成功駭入後再建立其管理員權限，從被揭露易遭受攻擊之 VPN 設備統計表，不乏 IP 位址設於台灣之主機，可見駭侵者仍伺機而動鎖定遠端連線設備之漏洞。

為強化 SSL VPN 之安全防護，以下將從 SSL VPN 部署提出建議，同時針對 SSL VPN 設備安全漏洞說明相關緩解措施。

2.1 SSL VPN 部署風險情境與改善建議

首先說明 SSL VPN 主要是基於 SSL(Secure Socket Layer)加密協定，於使用者與 SSL VPN 設備間建立一個安全加密連線通道，用戶端若使用瀏覽器與 SSL VPN 設備建立連線，則可免安裝 VPN 連線軟體。

常見 SSL VPN 設備分別有專屬硬體(Appliance)及整合式威脅管理 UTM(Unified Threat Management)防火牆兩種類型，專屬設備以特定軟體或硬體形式獨立運作與管理，UTM 防火牆則通常是以防火牆設備附加功能方式整合防火牆運作及管理。加密通道則有完全(Full)與分割(Split)兩種加密方式，說明如下：

- Full Tunneling 為 VPN 連線建立後，使用者所有對外網路流量均由此加密通道傳送至 SSL VPN 設備，包含上網與存取組織內部網路流量，使用者

上網行為可受組織防火牆與所建立之資安設備防護，可能造成之影響則為增加組織 Internet 之網路流量與降低使用者上網效能。

- Split Tunneling 因區隔不同通道，使用者與 SSL VPN 連線後，SSL VPN 所建立之通道只傳送存取組織內部網路之流量，若不經加密通道，則直接連接 Internet，因此組織 Internet 之網路流量與使用者上網效能皆不受影響，惟使用者上網行為亦無法獲得組織防火牆及資安設備之防護。

兩相比較，Full Tunneling 相較於 Split Tunneling 較具備安全性優勢，所有網路流量皆需通過組織之安全防護檢查，可與組織內部使用者達成一致性之安全防護基準，藉由組織之入侵防禦系統、網頁過濾及惡意中繼站連線阻擋等防護措施，加強使用者電腦安全性，同時組織亦可記錄與保存使用者完整之網路行為軌跡。

使用者與 SSL VPN 建立加密通道之後，對於內網服務有兩種存取模式，分別為門戶存取(Portal Access)與網路存取(Network Access)。Portal Access 意指使用者點選 Portal 頁面可用服務，由 SSL VPN 設備代理用戶端連線內網服務主機，代理連線以 Web 服務為主，使用者不會直接存取服務主機，確保服務主機之安全性；Network Access 由使用者與 SSL VPN 建立連線，取得一組虛擬網卡及 IP 位址後，將可直接存取內網服務主機，存取服務不限 Web 服務，SSL VPN 設備可藉由設定存取控制清單(Access Control List, ACL)，管控使用者網路連線及服務存取類型。

分析常見之 SSL VPN 部署常見錯誤樣態，大致可歸納為三種樣態：

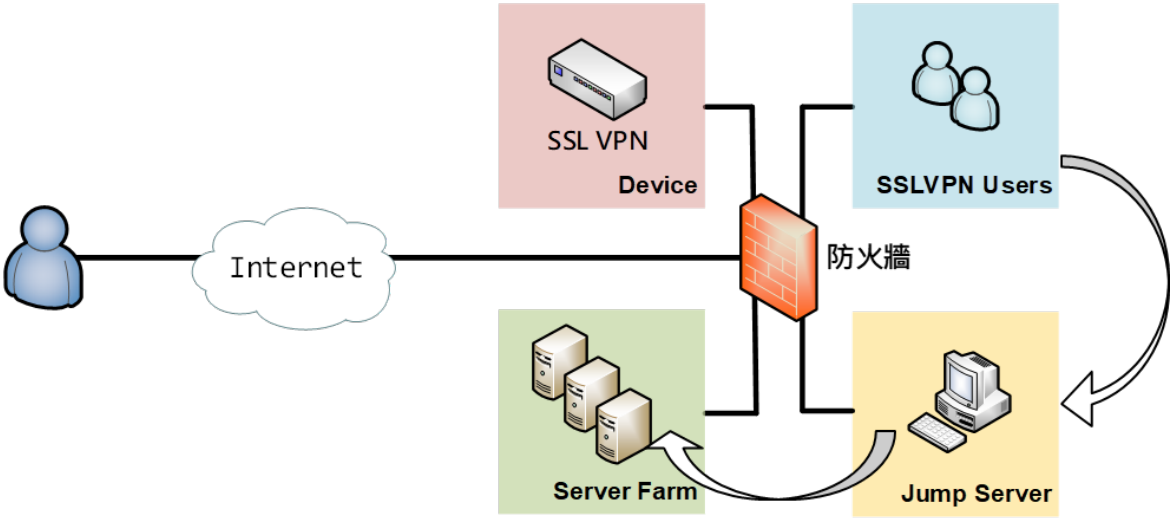
- 樣態一：SSL VPN 部署於防火牆外，服務存取點直接暴露於 Internet。常見發生之資安風險，可能因該設備存取不受防火牆保護，容易遭受阻斷服務攻擊(Denial-of-service, DoS)或漏洞利用攻擊。
- 樣態二：SSL VPN 部署於內網使用者區，分析其風險為 SSL VPN 使用者

因未規劃獨立網路區域，與內網使用者處於同一區域網路，若使用者電腦感染惡意程式，容易藉由 VPN 連線感染內網使用者，再擴權入侵內網伺服器。

- 樣態三：SSL VPN 部署於內網伺服器區，當使用者獲得授權連線後，Portal 或 Network Access 存取模式皆無法由防火牆提供防護及管控，因此使用者電腦感染惡意程式後，將輕易藉由 VPN 連線直接散播至內網伺服器。

綜整上述 3 種 SSL VPN 部署不同樣態，建議 SSL VPN 設備應部署於防火牆內部專屬區域，避免直接暴露於 Internet 可直接存取區域。而 SSL VPN 部署於防火牆內部專屬區域之目的，主要是運用防火牆與相關資安設備進行存取管控或資安防護，避免 SSL VPN 設備遭受非法存取與駭客攻擊。其次，設備管理介面與 SSL VPN 使用者應分開獨立部署於網路及防火牆專屬區域。若採用 Portal Access 模式，防火牆應禁止 SSL VPN 設備存取非授權之網路區域；採取 Network Access 模式時，防火牆應禁止 VPN 使用者存取 SSL VPN 設備與非授權之網路區域。

若 SSL VPN 設備組態設定可支援同時開啟 Portal 及 Network Access 模式，Portal Access 於存取 Web 應用服務時，應依使用者不同權限設定不同存取頁面，Network Access 存取則因無服務類型限制，管理者於防火牆組態設定時，應依使用者不同權限設定對應之存取政策，且於 Network Access 存取模式，另外再部署跳板機網路區域，要求 VPN 使用者須經由跳板機存取內網應用服務，則可更進一步透過防火牆加強 VPN 使用者與跳板機對內網服務之存取管控。綜合上述說明，SSL VPN 之部署建議示意圖詳見圖 4。



資料來源：本報告整理

圖4　SSL VPN 部署建議示意圖

2.2 SSL VPN 使用情境需求與設備漏洞緩解措施

SSL VPN 以往使用情境為因應臨時出差或短暫業務需求，現因疫情關係，遠距工作需求大增，同時遠端連線更轉為常態之工作模式。因此針對其連線之安全需求，首先應建置驗證使用者憑證之機制，若為內部使用者，可整合 AD 帳號，同時配合帳號密碼管理制度，登入時採用雙因子身分驗證，強化使用者身分鑑別或加入 CAPTCHA 驗證機制，避免機器人攻擊。而使用者設備鑑別部分，應鎖定其設備 MAC Address 或連線之 IP 位址，並定期要求執行設備安全檢查。

近年來已揭露之 SSL VPN 設備安全漏洞類型，主要以可遠端執行任意程式碼(RCE)為主，相關風險皆列為嚴重或高危險等級，且常見知名網通品牌因其產品漏洞所導致之資安事件，統計常見之部分漏洞清單，詳見表 1。

表1　SSL VPN 設備安全漏洞列表

公布時間	CVE 編號	漏洞種類	危險等級	修補結果
2019/12/27	CVE-2019-19781	允許遠端執行任意程式碼	嚴重	已提供修補
2019/10/02	CVE-2019-12677	DoS 攻擊弱點	中	已提供修補
2022/05/04	CVE-2022-1388	允許遠端執行任意程式碼	嚴重	部分版本未提供修補
2022/04/28	CVE-2021-23008	身分驗證漏洞	嚴重	部分版本未提供修補
2019/06/04	CVE-2018-13379	未經驗證的任意讀檔	嚴重	已提供修補
2021/11/11	CVE-2021-3064	允許攻擊者執行系統命令進而接管系統及遠端執行任意程式	嚴重	已提供修補
2021/04/20	CVE-2021-22893~22894	允許遠端執行任意程式碼	嚴重~高	已提供修補
2019/05/08	CVE-2019-11510	未經驗證的任意讀檔	嚴重	已提供修補
2021/01/23	CVE-2021-20016	允許遠端執行任意程式碼	嚴重	已提供修補

資料來源：本報告整理

面對 SSL VPN 設備相關漏洞可能造成之風險，即時修補為最有效且直接之解決方案。政府機關應有漏洞偵測與揭露之相關程序，且建立安全漏洞訊息處理機制，於接獲相關設備之漏洞警訊後，立即評估對業務之衝擊分析，並規劃執行修補作業。設備廠商通常對於被外部揭露或自我發現之設

備安全漏洞，於技術支援期間內，皆會釋出相關漏洞修補程式與緩解措施。若因韌體版本或內部應用服務相容性而無法進行系統修補者，則應儘速評估其風險，採取其他緩解或補償控制措施以確切降低風險。面對 SSL VPN 設備之漏洞，整理常見漏洞緩解作法，詳見表 2。

表2　SSL VPN 設備漏洞常見緩解作法

編號	緩解作法	適用之安全漏洞範例
1	修改系統組態設定	CVE-2019-19781 CVE-2022-1388 CVE-2021-22893
2	停用受漏洞影響的系統服務	CVE-2018-13379
3	禁止存取受漏洞影響之服務路徑	CVE-2022-1388
4	啟用 WAF 或 IPS 關於漏洞之防護	CVE-2021-3064 CVE-2021-20016
5	加強身分鑑別，採用多因子驗證機制	CVE-2021-23008 CVE-2021-20016

資料來源：本報告整理

機關應就本身所使用之設備，檢視其身分驗證機制、組態設定、服務埠開啓之必要性及強化遠端連線資安防護與監控作為。除安全性修補與緩解措施外，強化 SSL VPN 設備管理與安全之網路部署，可有效降低漏洞被利用與攻擊風險。

3.資安技術研析_AD 攻擊手法研析與 CVE 弱點驗證實作

本季探討之資安技術研析為目錄伺服器(Active Directory, AD)攻擊手法研析與 CVE-2022-26923 權限提升弱點驗證實作，有鑑於 AD 伺服器擔負網域管理與權限存取之功能，如 AD 可透過群組原則，大量部署管理原則與管理電腦之組態設定，同時透過 AD 之帳號集中管理機制，整合不同資通系統驗證程序，可讓使用者運用單一登入方式，減少記憶不同帳號密碼之程序，從資安整備度來看，AD 向來為資安之基礎防護重點標的，因攻擊者若成功入侵 AD，即可控制整個網域並存取相關主機服務，如電子郵件或人事管理等資通系統。

以下將研析常見針對 AD 之攻擊手法，彙整近年遭攻擊者所利用弱點，並就 111 年揭露之 CVE-2022-26923 權限提升弱點進行實作驗證，分析其入侵手法，並提供弱點修補建議。

3.1 AD 弱點成因與實作

分析 AD 攻擊流程，攻擊者會採取先攻陷外網主機策略，嘗試先攻擊位於非軍事區(Demilitarized Zone, DMZ)等對外提供服務網段之高風險主機，進行本地權限提升與內部橫向移動，以伺機取得 AD 主機控制權，再利用 AD 管理者權限取得機敏資訊或散布。以下列舉 109 到 111 年 AD 重大弱點，並說明其相關風險。首先說明弱點 CVE-2020-1472(ZeroLogon)，該弱點利用 Netlogon 權限提升漏洞，透過修改 Netlogon 協定中加密演算法之參數，可成功通過伺服器身分驗證，進而取得網域控制權。另外，有數個通報為 AD 網域權限提升之弱點，如 CVE-2021-42278、CVE-2021-42282 等。而透過 AD 遠端執行任意程式碼弱點，則有 CVE-2020-0718、CVE-2020-0761 等利用目錄伺服器集成網域名稱系統(Active Directory Integrated DNS, ADIDNS)弱點，可在 AD 網域上遠端執行程式碼。

由美國非營利機構 MITRE 統計 ATT&CK 矩陣之 AD 相關攻擊技術，包含從持續潛伏至衝擊等戰術中，共有 14 種不同類型攻擊技術，其中又以權限提升、憑證存取及橫向移動為關鍵戰術，詳見圖 5。

持續潛伏	權限提升	防禦逃脫	憑證存取	發現	橫向移動	衝擊
Account Manipulation	Domain Policy Modification	Use Alternate Authentication Material (Pass the Hash, Pass the Ticket)	Steal or Forge Kerberos Tickets (Golden Ticket, Kerberoasting, AS-REP Roasting)	Group Policy Discovery	Use Alternate Authentication Material (Pass the Hash, Pass the Ticket)	Account Access Removal
Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Domain Policy Modification	OS Credential Dumping (DCSync)	System Owner/User Discovery		
Modify Authentication Process	Access Token Manipulation	Access Token Manipulation	Modify Authentication Process			
Create Account		Rogue Domain Controller				
		File and Directory Permissions Modification				
		Modify Authentication Process				

資料來源：https://attack.mitre.org/datasources/DS0026/

圖5　ATT&CK 矩陣之 AD 相關攻擊技術

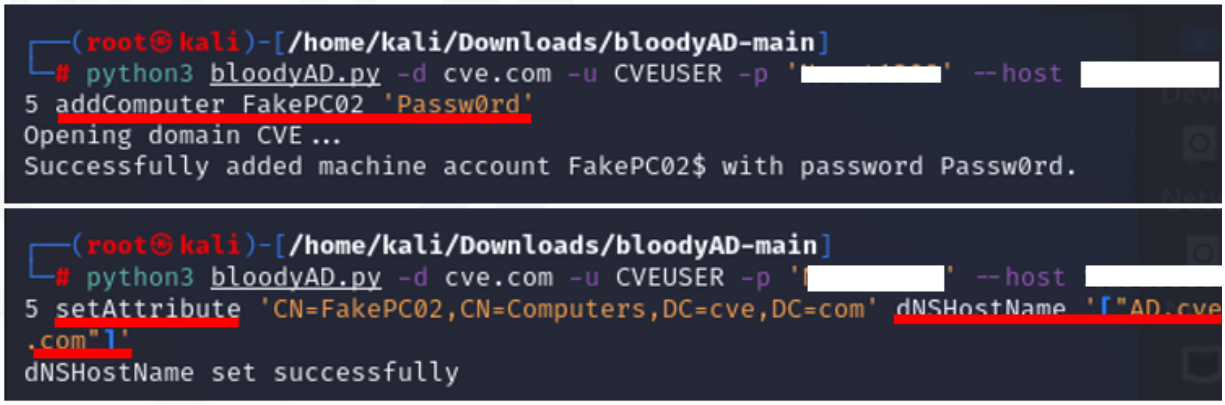
分析駭客行為模式發現其為達成戰術目標，通常會先搜尋可利用之弱點，因此若能針對弱點進行分析且進一步了解 AD 伺服器可能遭攻擊路徑，將有助於快速辨識 AD 之異常狀況，避免不當提權或橫向擴散之風險，因此本報告接續針對近期所發布之 CVE-2022-26923 弱點進行概述與實作驗證。此弱點影響範圍為所有版本之 Windows Server，且 CVSS 分數高達 8.8，藉由弱點驗證實作結果，可應用於未來網路攻防演練、技術檢測或跨國攻防演練場域之攻擊手法與途徑設計。CVE-2022-26923 弱點主要由於電腦帳戶所使用 DNS Host Name(dNSHostName 參數)不具有唯一性，攻擊者可進行偽冒，將其修改成特權網域電腦帳戶之 dNSHostName，接續利用 AD 憑證服務(Active Directory Certificate Service, AD CS)使用

dNSHostName 識別電腦身分之特性獲得特權憑證，再以特權憑證進行 Kerberos 驗證後，即可取得網域控制權。實作驗證環境模擬建置，詳見圖 6。

資料來源：本報告整理

圖6　實作驗證環境

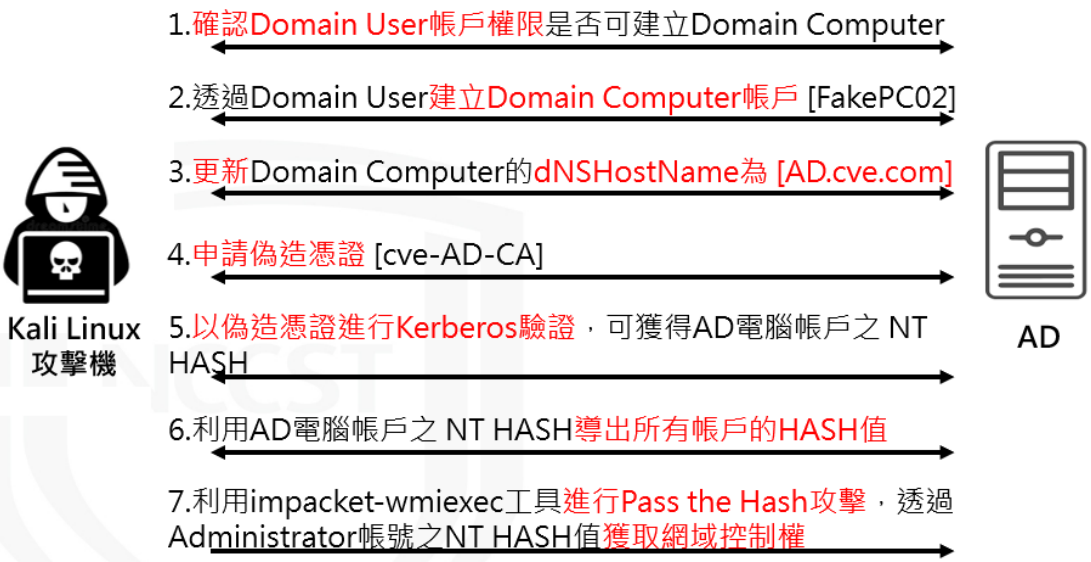
實作環境建立後，首要步驟為確認 Domain User 帳戶權限是否可建立網域電腦 Domain Computer (ms-DS-MachineAccountQuota > 0)，接續透過網域使用者 Domain User 建立 Domain Computer 帳戶[FakePC02]，且更新 Domain Computer 之 dNSHostName 為[AD.cve.com]，詳見圖 7。



資料來源：本報告整理

圖7　建立 Domain Computer 帳戶

透過申請偽造憑證[cve-AD-CA]，並以偽造憑證進行 Kerberos 驗證，成功獲取 AD 電腦帳戶之 NT HASH，再利用 AD 電腦帳戶之 NT HASH 推導出所有帳戶 HASH 值。最後步驟於實作環境中利用 impacket-wmiexec 工具進行 Pass the Hash 攻擊，透過 Administrator 帳號之 NT HASH 值獲取網域控制權。整體弱點驗證實作步驟，詳見圖 8。

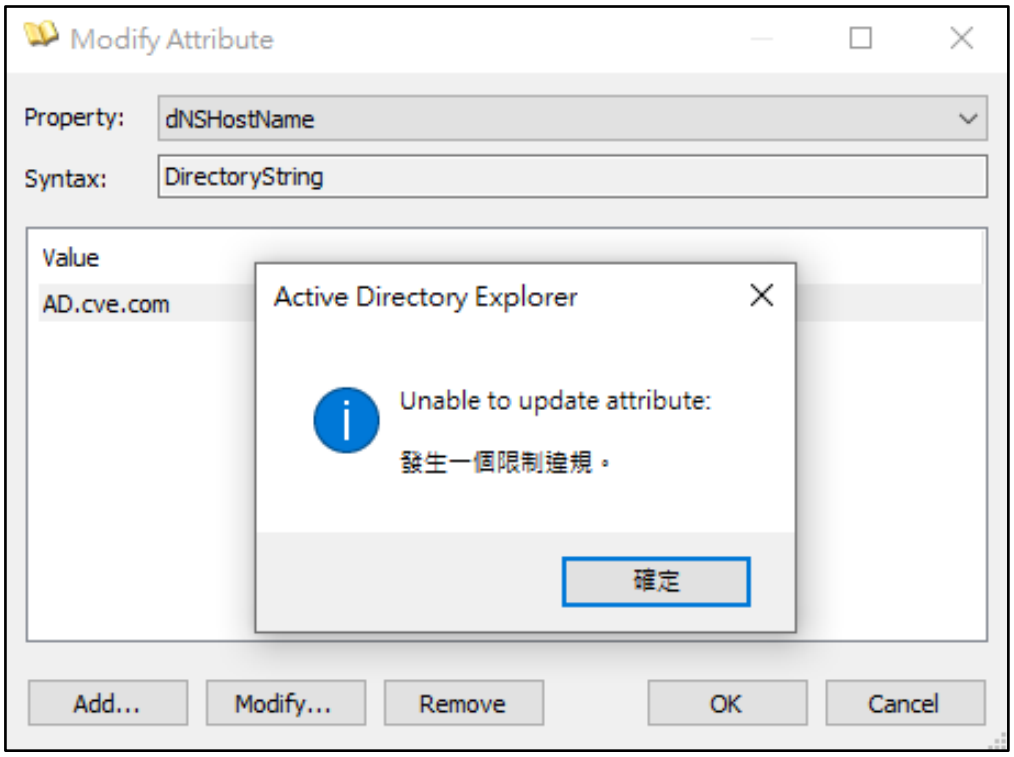


資料來源：本報告整理

圖8　弱點驗證實作步驟

3.2 CVE-2022-26923 弱點修補方式

微軟已提供 CVE-2022-26923 修補程式，惟因陸續出現更新導致某些服務驗證失敗之問題，官方再次釋出新版修補程式，修補方式為提升修改屬性所需權限，改為至少需網域管理者(Domain Admin)層級之帳戶權限才可修改屬性，針對已修補此弱點之 AD 以 Domain User 權限修改屬性時，會出現錯誤訊息，詳見圖 9。



資料來源：本報告整理

圖9　以 Domain User 權限已無法修改 dNSHostName 屬性

另外，修補程式亦於憑證中導入名為「szOID_NTDS_CA_SECURITY_EXT」之新物件 ID(Object ID, OID)，藉由在該 OID 中嵌入安全性識別碼(SID)以進一步對用戶進行身分驗證。若以相同攻擊手法申請偽造之憑證，驗證後會發現該憑證之 SID 與使用者 SID 不匹配，詳見圖 10。

資料來源：本報告整理

圖10 驗證 Object_SID

由此弱點可得知，若非業務必要，管理者預設不應安裝憑證服務(CS)。其他管理與因應措施包含設定憑證範本權限，確保僅在業務需要時，才允許註冊電腦憑證範本。如此可成功攔阻欲透過電腦憑證範本申請偽造憑證之攻擊手法，詳見圖 11。

資料來源：本報告整理

圖11 設定憑證範本權限攔阻偽造憑證

其他管控措施亦可透過管理 Domain User 限制建立 Domain Computer 之數量，將 ms-DS-MachineAccountQuota 設置為 0，非必要不允許其新增 Domain Computer，或藉由套用政府組態基準(Government Configuration Baseline, GCB)，將電腦設定\Windows 設定\安全性設定\具有進階安全性之 Windows 防火牆之輸入連線預設為封鎖，如此皆可加強 AD 組態設定之安全性以避免此項攻擊。

4. 結論

本季具指標性案例為Microsoft IIS Web 伺服器之日誌遭駭客運用於操控惡意程式，駭客組織 Cranefly 運用新興技術，藉著通過 Microsoft Internet Information Services (IIS) Web 伺服器日誌，達到控制受感染設備上惡意程式之目的。另一起案例為美國某家媒體公司因遭駭客入侵，引發後續供應鏈攻擊危機，因該媒體公司主要提供影音內容與廣告予其他媒體新聞網站，駭客藉由竄改 JavaScript 之基礎程式碼，進而部署惡意程式，偽冒假更新至逾 250 家新聞網站，因此引發一波供應鏈供擊之風波。

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」類型為主，排除綜合類型「其他」外，其次分別為「設備問題」與「網頁攻擊」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「新興攻擊趨勢與手法之資安管理」與「設備鑑別與可靠性之資安管理」提出資安防護建議。

資安專題分享主題為 SSL VPN 安全部署，針對駭客持續查找 VPN 設備之最新漏洞，藉此竊取憑證或橫向入侵，可強化 SSL VPN 之安全防護，建議 SSL VPN 設備部署於防火牆內部專屬區域，避免直接暴露於 Internet 可直接存取區域。其次，設備管理介面與 SSL VPN 使用者應分開獨立部署於網路及防火牆專屬區域。同時針對 SSL VPN 設備安全漏洞說明相關緩解措施，面對 SSL VPN 設備相關漏洞可能造成之風險，即時修補為最有效且直接之解決方案。

另外，資安技術研析主題為 AD 攻擊手法研析與 CVE 弱點驗證實作，AD 擔負網域管理與權限存取之功能，向來為資安之基礎防護重點標的，攻擊者若成功入侵 AD，即可控制整個網域並存取相關主機服務，如電子郵件或人事管理等資通系統。本次研析主題說明 AD 之常見攻擊手法，並彙整近年遭攻擊者所利用弱點，且就 CVE-2022-26923 權限提升弱點進行實作

驗證，分析其入侵手法，並提供弱點修補建議。

資安相關活動

本季數位發展部資通安全署辦理之資安相關活動，說明如下。

◆ 111 年國家資安資訊分享與分析中心(N-ISAC)年會

N-ISAC 年會於 11 月 28 日假台大醫院國際會議中心辦理，議程除安排 N-ISAC 111 年執行情形與 STIX2.1 推動說明報告外，亦安排 2 個專題報告，分別為年度資安威脅回顧與未來挑戰、亞太地區網路攻擊活動趨勢與案例研析。另外，從議題引言從關鍵基礎設施及支援運作之核心服務改善推動目標與規劃，接續分組討論加強機關(構)資安防護能量之實務作法與精進規劃。

N-ISAC 111 年執行情形包含分享領域內資安事件與攻擊活動之研析報告，強調應持續加強跨領域資安聯防，同時透過產製資安事件情資需具備之資安監控與分析能量，將惡意行為及時應處並通知受駭單位。專題報告提及因台灣政經地緣等關係，遭遇諸多攻擊，且因新式攻擊手法盛行，如新興勒索軟體與目標式攻擊，資安防護整備程度亦應持續強化。專題報告整理未來挑戰包含滲透測試與開源工具普及，導致攻擊事件發動相對簡單、攻擊行為轉變之挑戰，不僅目標式攻擊大幅增加，對象亦不限定機敏單位等。分組討論之重點從如何落實資安管理政策、強化外部威脅防禦及精進內部資安管理等議題進行討論。

◆ 111 年第 2 次政府資通安全防護巡迴研討會

第 2 次政府資通安全防護巡迴研討會於 11 月至 12 月期間辦理，分別於台北、台中、高雄及台東等地共辦理 8 場研討會。政府資通安全防護巡迴研討會主要針對資通安全管理法納管對象之資安專職(責)人員，期許透過研討會方式宣導政府機關資安威脅與防護重點、分享資安稽核常見待改善事項及建議作法，同時對於 110 年網路攻防演練暨資安檢測所發現之重要事

項，進行共同發現事項之根因探討，並提供修正建議。

議題一政府機關資安威脅與防護重點，分享全球與資通安全威脅趨勢，對於相關威脅趨勢，規劃資安防護強化重點，如配合資通安全管理法，符合其所屬資通安全責任等級之要求，落實資通安全防護應辦事項，以因應六大類資通安全威脅情勢變化，並需特別強化郵件安全與防護整備及落實資產管理與弱點修補等建議事項。議題二資安稽核常見待改善事項，包含未落實核心業務與核心系統之界定或機關囿於資安人力資源，未妥善配置資安專職/責人力，以及針對資通系統所使用之外部元件或軟體，缺乏更新、管控機制等。議題三 111 年網路攻防演練暨資安檢測歸納揭露之弱點，包含參數遭猜測與限制存取功能失效，屬於無效之存取控管；未落實通行碼強度檢查機制，顯示認證及驗證機制失效；網頁功能頁面未限制存取等不安全之組態設定等為政府機關常見弱點。