110年第1季資通安全技術報告

Quarterly Technical Report

目　次

1. 資安威脅現況與防護重點 3
1.1 全球資安威脅現況 3
1.2 政府資安威脅現況 4
1.3 資安防護重點 7
2. 資安專題分享_零信任網路設備鑑別簡介 9
2.1 零信任網路設備鑑別技術 9
2.2 零信任網路設備鑑別架構與驗證 10
3.資安技術研析_ Cobalt Strike 後門程式/中繼站調查分析 14
3.1 情蒐分析與研究調查流程 14
3.2 Cobalt Strike 連線中繼站後續追蹤與監控 17
4. 結論 19

圖 目 次

圖 1　110 年第 1 季通報事件影響等級比率圖 5
圖 2　110 年第 1 季通報類型比率圖 6
圖 3　110 年第 1 季公務機關資安事件原因比率圖 7
圖 4　設備健康管理流程 10
圖 5　零信任網路設備鑑別架構 11
圖 6　基於 TPM 設備鑑別實作 PoC 架構 12
圖 7　設備健康管理實作 PoC 架構 12
圖 8　設備健康日誌 13
圖 9　Cobalt Strike 後門程式之情蒐分析與研究調查流程 15
圖 10　Cobalt Strike 連線中繼站匿蹤技術之 3 種樣態 16
圖 11　偽冒 DC 身分與 DC 建立安全通道 17

摘要

「第 1 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，提供政府機關最新資安風險之關注重點。

「第 1 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 起案例為美國佛羅里達州淨水處理廠遭駭客入侵；第 2 起案例為資安業者揭露 NoxPlayer 供應鏈攻擊行動。

分析政府資安威脅現況，發現政府機關通報事件，以「非法入侵」(占 78.75%) 類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 7.5 %)」與「網頁攻擊(占 2.5%)」為主要通報類型。

●2.資安專題分享

資安專題分享主題為零信任網路設備鑑別簡介，零信任網路無信任邊界概念，在於資訊存取不因設備所在網路位置而產生不同信任程度，其中設備鑑別與健康管理是零信任網路核心需求之一。針對零信任網路之設備鑑別方法與健康管理流程進行說明，並進行相關技術概念性驗證。

●3.資安技術研析

資安技術研析主題為 Cobalt Strike 後門程式/中繼站調查分析，109 年政府機關資安事件，發現駭客常使用 Cobalt Strike 做為攻擊工具。駭客除透過社交工程惡意電子郵件散布後門程式，亦使用 HTTP(S)或 DNS 隧道通訊等加密技術，偽冒合法網站隱藏中繼站(Team Server)連線資訊，進行資料竊取。

●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。資安專題分享零信任網路設備鑑別簡介，概述零信任網路之設備鑑別方法與健康管理流程，並進行相關技術概念性驗證。此外，資安技術研析主題為 Cobalt Strike 後門程式/中繼站調查分析，包含情蒐研究方法與調查流程，並針對 Cobalt Strike 連線中繼站進行後續追蹤與監控。

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。110 年第 1 季(以下簡稱本季)探討供應鏈安全與如何加強資通系統防護，以避免遭受攻擊致資料外洩。

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

全球因疫情關係，許多經濟活動受影響因而遲緩或停頓，但資安事件仍頻傳且居高不下，如駭客組織運用惡意軟體入侵，控制受駭電腦並形成大型殭屍網路，擴大其影響範圍。其中，不容輕看之事件是對於關鍵基礎設施之危害。關鍵基礎設施一旦因駭客入侵停止運作或降低效能，對國家安全、公共利益、國民生活或經濟活動將產生重大影響。因此，應特別關注關鍵基礎設施資安防護，持續監控其維運架構可能風險與發生之資安事件。

本季具指標性案例為美國佛羅里達州淨水處理廠遭駭客入侵；另一起案例為資安業者揭露 NoxPlayer 供應鏈攻擊行動。

首先，探討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 109 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。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。

根據調查，事件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 TeamViewer、未安裝防火牆防護及共用密碼等不安全使用行為。該淨水處理廠除使用微軟已於 109 年終止支援之 Windows 7 作業系統，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。

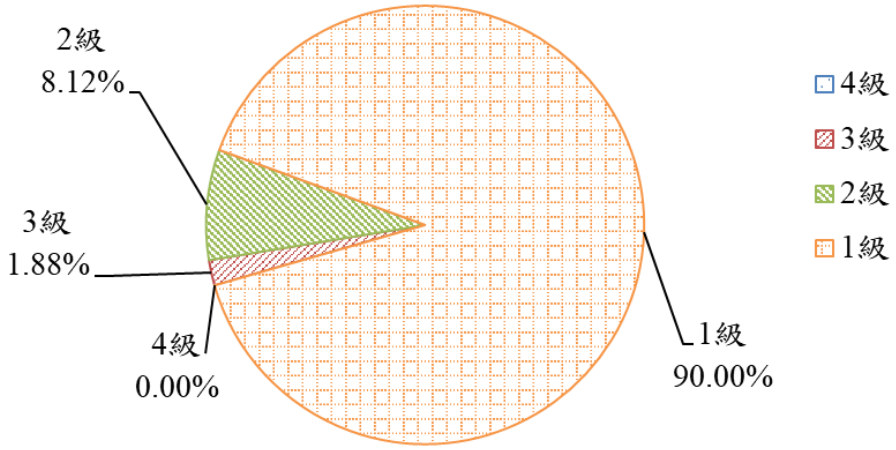
第 2 起案例為資安業者 ESET 揭露，針對知名 Android 遊戲模擬器 NoxPlayer 之供應鏈攻擊行動，受駭範圍包含台灣、香港及斯里蘭卡等國。NoxPlayer 為 BigNox 開發之遊戲模擬器，宣稱於全球擁有 1.5 億個用戶，主要來自於亞洲地區。

ESET 將此波攻擊行動命名為「Operation NightScout」，109 年 9 月駭客開始透過 NoxPlayer 更新機制，於用戶執行更新時植入惡意程式，該惡意程式主要用途為蒐集用戶資訊，包含用戶鍵盤輸入紀錄與機敏資訊等。

綜覽本季重大資安事件，關鍵基礎設施之風險議題應特別關注，落實相關資安準則與資通安全維護計畫，以符合其資安防護等級。透過供應鏈攻擊，不論是藉由資通訊服務或更新機制進行攻擊之事件已屢見不鮮，因此於開通相關資通訊服務或更新前，應進行風險分析，辨識相關風險，確認可接受風險程度。

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 90%為大宗，2 級事件占 8.12%次之，3 級事件僅占 1.88%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

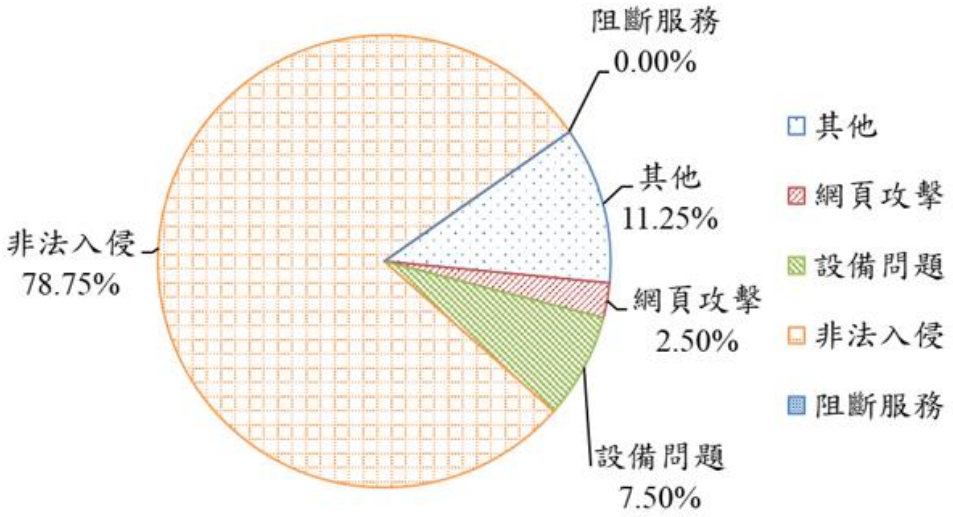


資料來源：本報告整理

圖1　110 年第 1 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，大多為個人資料外洩事件，包含對外報名系統存在網頁上傳漏洞，致遭駭客利用進而上傳惡意程式，之後更進一步入侵內部資通系統，成功竊取該系統儲存之個人資料。另一起個人資料外洩事件，則因政府機關辦理活動，委外廠商不慎將民眾登錄參與活動之資料放置於公開活動網站，且未進行資料遮蔽，經調查活動頁面已被瀏覽點擊數十次，恐有數萬筆個人資料遭洩漏之虞。

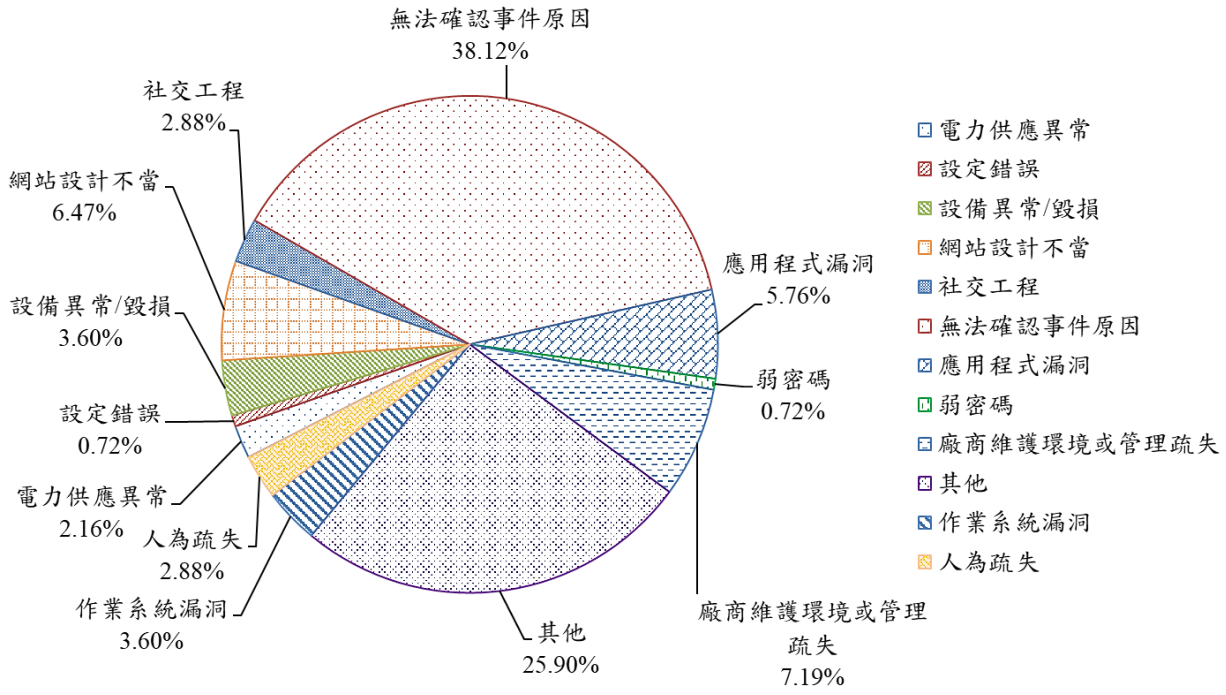
除上述資安事件外，技服中心偵測多個機關連線行為符合鍵盤側錄惡意程式(keylogger)連線特徵，部分機關調查判斷鍵盤側錄程式係經由隨身碟植入至受駭設備，其餘機關則無法確認惡意程式植入原因。非法入侵在政府機關資安事件比率，有逐步升高之趨勢，值得深入研究發生肇因，由源頭緩減非法入侵風險。整體事件比率，以「非法入侵」(占 78.75%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　110 年第 1 季通報類型比率圖

接續，分析通報事件發生之原因(詳見圖 3)，可確認之事件原因分別為廠商維護環境或管理疏失(7.19%)、網站設計不當(6.47%)、應用程式漏洞(5.76%)、設備異常/毀損(3.6%)、作業系統漏洞(3.6%)、社交工程(2.88%)、人為疏失(2.88%)、電力供應異常(2.16%)、設定錯誤(0.72%)及弱密碼(0.72%)。統計本季事件發生原因，發現「弱密碼」由上季(13.82%)大幅下降至不到 1%，顯示密碼設定之安全性已被使用者重視。此外，分析「廠商維護環境或管理疏失」，發現機關因資通系統委由廠商維護管理，駐點廠商使用其自有設備，卻未遵守機關設備使用規範，如確保作業系統需定期更新、禁用遠端存取軟體及安裝防毒軟體等防護措施，致產生資安風險。



資料來源：本計畫整理

圖3　110 年第 1 季公務機關資安事件原因比率圖

1.3 資安防護重點

分析本季全球資安威脅現況，關鍵基礎設施顯然已成為駭客鎖定之攻擊目標，姑且不論其攻擊原因為何，關鍵基礎設施一旦遭入侵成功，影響甚鉅，因此更應加強其資安防護強度，全面進行資安檢測，以及早發掘潛在弱點。以風險管理為基礎之資安防護概念，除針對內部防護外，對於外部供應鏈之風險辨識更應加強，以因應內外之資安攻擊。

技服中心偵測到多個機關連線行為符合鍵盤側錄惡意程式連線特徵，有部分機關為經由隨身碟植入至受駭設備。隨身碟因輕巧且使用方便，惟其遭受惡意程式感染之風險高，尤其此次之鍵盤側錄惡意程式，若未能及早發現，可輕易竊取使用者電腦資料。

綜整以上資安威脅現況，提供資安防護建議如下：

●關鍵資訊基礎設施資安管理

– 建構嚴謹之工控場域網路區隔，關閉不必要之通訊埠。

– 建立嚴謹之存取控制配置清單，定期進行審查，非必要不開放遠端連線存取。

– 密切關注重大工控安全性漏洞及修補訊息，需對漏洞修補進行嚴格之安全評估與測試驗證。

●系統自動更新之資安管理

– 僅透過 HTTPS 提供更新軟體，降低域名劫持(Domain Hijacking)與中間人攻擊之風險。

– 透過 MD5 雜湊值與檔案簽名，以檢視其完整性。

– 其他資安管理措施，如惡意軟體偵測機制或機敏資訊加密等。

●隨身碟之資安管理

– 僅允許使用登錄造冊之隨身碟存取，且使用前應進行安全掃描。

– 不得儲存機敏資料，若需儲存應啟動加密機制，並監控其留存狀況。

– 加強端點防護機制，即時偵測且快速阻絕擴散之可能。

2. 資安專題分享_零信任網路設備鑑別簡介

隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統以信任邊界所形成之網路架構已無法因應無所不在之資安威脅。為此，美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)發布 NIST SP 800-207 零信任架構(Zero Trust Architecture)，指出政府與組織應推動使用零信任網路，以因應遠距工作與雲端存取之趨勢。109 年第 1 季報告中，已簡介零信任網路之架構與身分鑑別、設備鑑別及信任推斷等 3 項關鍵技術。在本報告中，將進一步針對零信任網路之設備鑑別與健康管理進行說明。

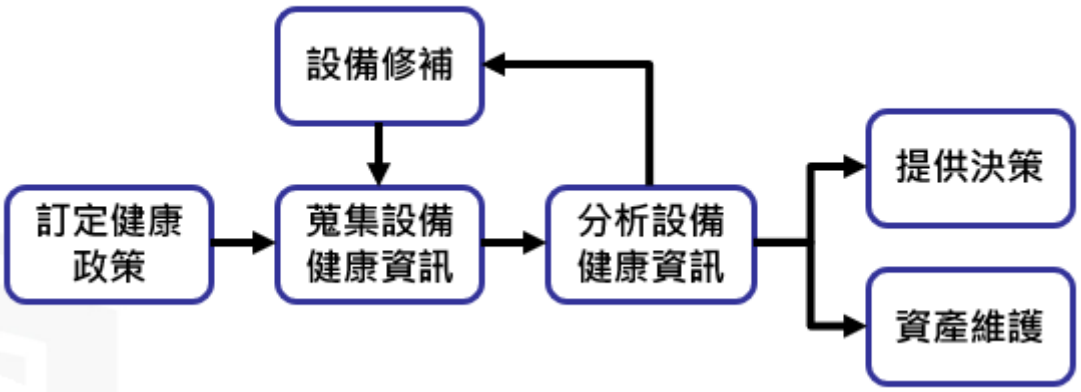
設備鑑別之目的在於識別所使用之設備是否為受管理之設備，而設備健康管理則用於確保所使用之設備維持在可接受之資安狀態。以下針對零信任網路之設備鑑別方法與健康管理流程進行說明，並針對相關技術進行概念性驗證(Proof of Concept, PoC)。

2.1 零信任網路設備鑑別技術

實施設備鑑別可防止未知或未受管理之設備存取資通系統，以避免機敏資訊遭洩漏，或無法於資安事件發生時即時追溯根源。設備鑑別有 2 種方法，分別為基於信賴平台模組(Trusted Platform Module, TPM)與基於短暫金鑰(Limited Use Credential, LUC)。TPM 適用於內嵌安全晶片之設備，如微軟與 Apple 之設備安全解決方案，而 TPM 為 Windows 10 之必要硬體需求，主要利用安全晶片密碼模組與金鑰管理機制執行鑑別協議，如基於憑證之 TLS 客戶端鑑別(Certificate-based TLS Client Authentication)。LUC 適用於無安全晶片之設備，如 Android 行動裝置等，主要利用線上金鑰管理伺服器隨時更新短暫金鑰，執行鑑別協議，如三方金鑰交換(Three-Party Key Exchange)等。

實施設備健康管理可確保與追蹤設備之資安狀態，以避免具有漏洞或惡意

程式之設備存取資通系統，降低資安風險，設備健康管理流程詳見圖 4。



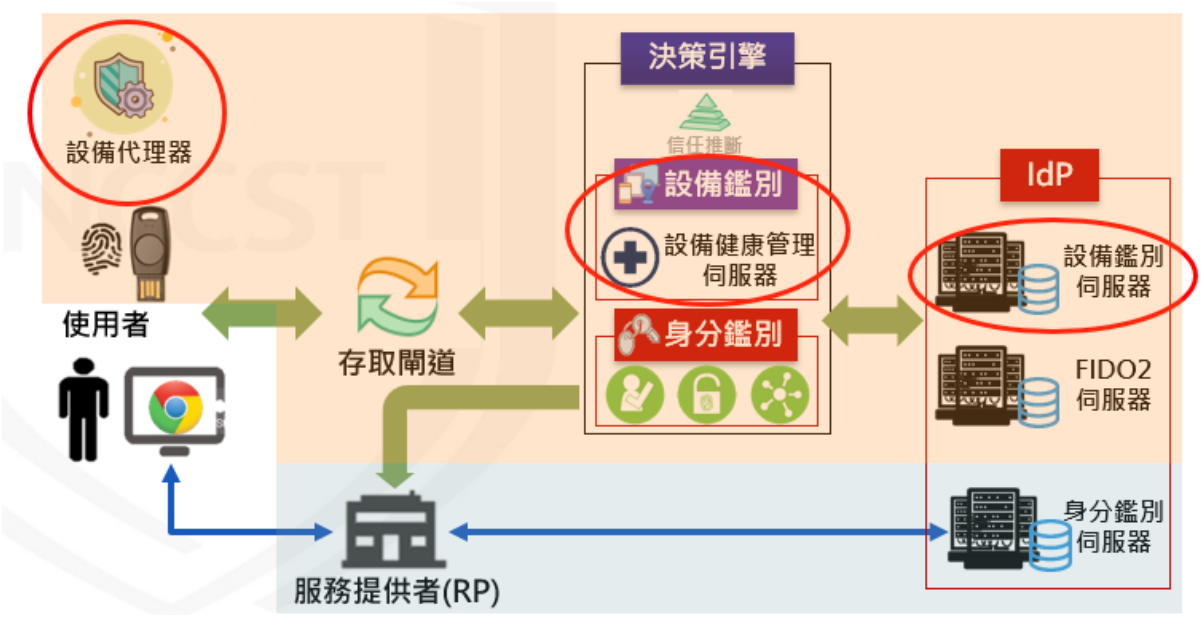
資料來源：本報告整理

圖4　設備健康管理流程

首先訂定健康政策，定義可接受之資安規則或狀態。其次為蒐集設備健康資訊，設計與執行蒐集指令，排程蒐集腳本。接續分析設備健康資訊，依健康政策檢驗健康狀態，如日誌分析與異常偵測等。之後設備修補階段，針對健康狀態不合格之設備，進行組態調整或軟體更新。最後依據設備健康管理結果，提供設備健康狀態，以進行信任推斷與存取授權，並依設備健康狀態，維護資產管理資料庫紀錄。

2.2 零信任網路設備鑑別架構與驗證

本節將以開源軟體為主，於零信任網路中規劃設備鑑別架構，並進行 PoC 以驗證其可行性，包含建置設備代理器(設備鑑別與健康管理)、設備健康管理伺服器及設備鑑別伺服器，詳見圖 5。



資料來源：本報告整理

圖5　零信任網路設備鑑別架構

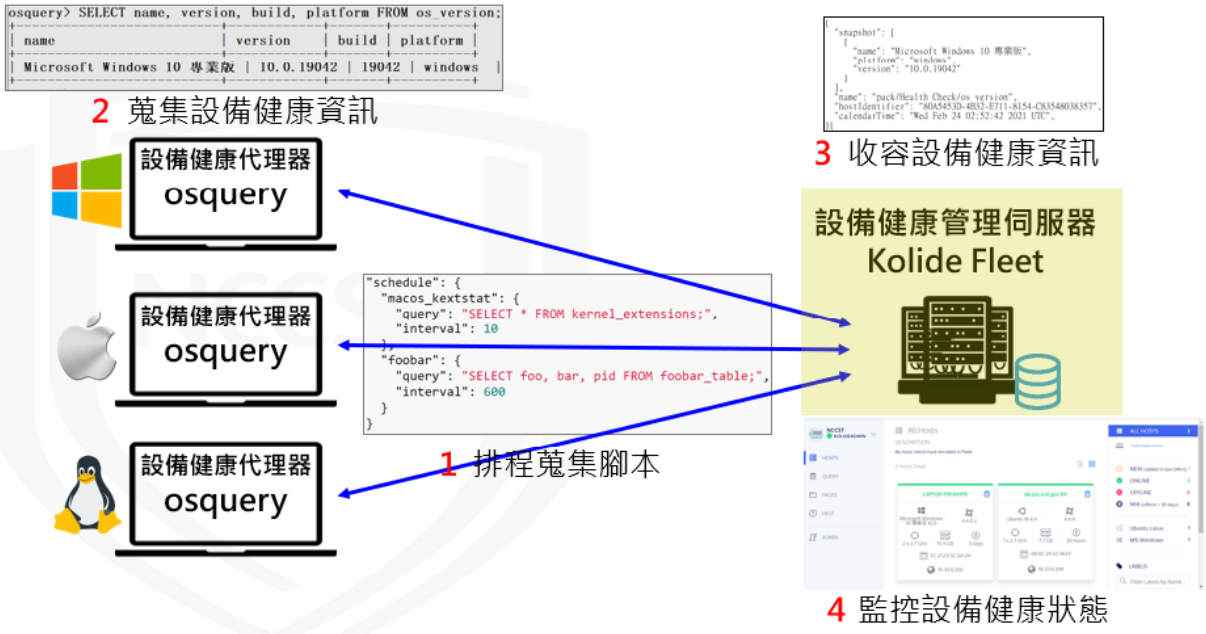
設備鑑別採用 TPM 方法，TPM 安全機制是基於受硬體保護之金鑰管理，TPM 製造時，會產生唯一之 Seed 存於 TPM 之防竄改非揮發性記憶體(Tamper-Proof Non-Volatile Memory)，Seed 再透過金鑰衍生函數(Key Derivation Function, KDF)產生 RSA 或 ECC 主金鑰對(Primary)與公鑰憑證。TPM 應用時，可依應用產生 RSA 或 ECC 之子金鑰，公鑰(Public)可依應用由 CA 簽發 X.509 憑證，私鑰(Private)匯出受父金鑰加密(Enc)保護。

在 PoC 實作上，於設備鑑別客戶端，利用 OpenSSL 之 TPM 引擎，經由 TPM2-TSS(TPM Software Stack)呼叫 TPM 密碼模組，產生設備 RSA 金鑰，進行設備鑑別所需之簽章運算；CA 則利用 OpenSSL 對設備之 RSA 公鑰簽發設備憑證；設備鑑別伺服器則利用 OpenSSL 驗證設備鑑別之簽章，詳見圖 6。

資料來源：本報告整理

圖6　基於 TPM 設備鑑別實作 PoC 架構

而在設備健康管理部署 PoC，設備健康代理器挑選使用 Facebook osquery 開源碼系統管理工具以蒐集設備健康資訊，並建置 1 台 Windows 10 與 1 台 Linux Ubuntu；設備健康管理伺服器則利用 Kolide Fleet 以收容與監控設備健康資訊，並以圖形化介面監控連線設備，完整實作 PoC 架構，詳見圖 7。



資料來源：本報告整理

圖7　設備健康管理實作 PoC 架構

本次 PoC 實作範圍主要為蒐集設備健康資訊，首先建立蒐集指令，分別蒐集作業系統、設備識別及系統安全性資訊，並利用排程蒐集腳本與設備健康資訊，每 30 分鐘執行 3 項排定之蒐集指令。最後，建立設備健康日誌，以 JSON 格式儲存設備健康日誌，以利後續分析，詳見圖 8。

資料來源：本報告整理

圖8　設備健康日誌

零信任網路資安防護架構規劃，係依據第六期國家資通安全發展方案之主動式防禦策略進行研析，藉由發展主動式防禦技術，建立零信任網路資安防護驗證環境，後續將持續研析零信任網路之信任推斷技術，以完善整體網路防禦縱深機制。未來，亦將逐步推動政府機關導入零信任網路資安防護架構，以強化資安防護能力。

3.資安技術研析_ Cobalt Strike 後門程式/中繼站調查分析

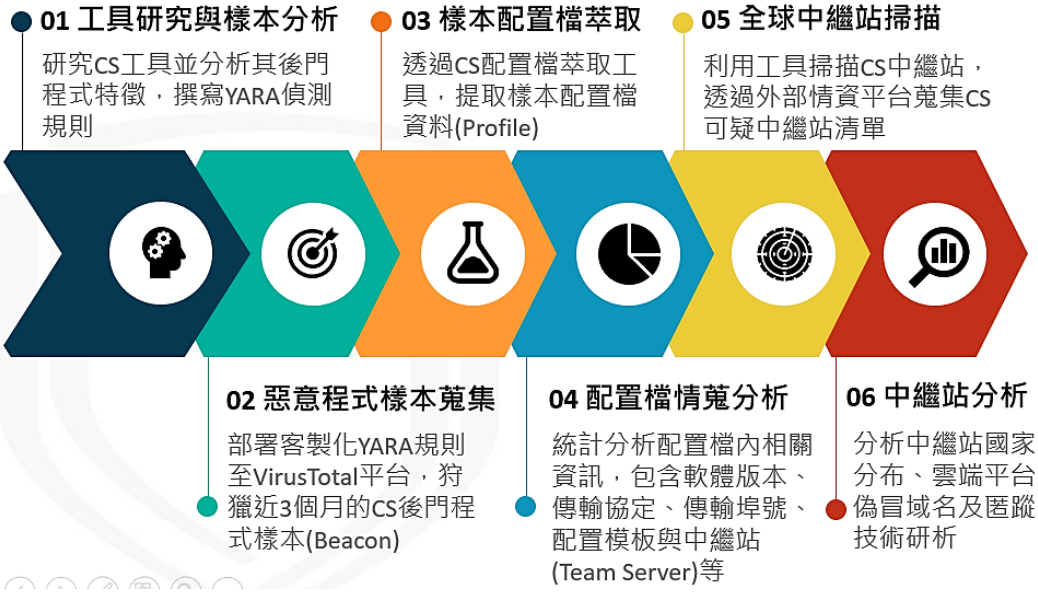
本季探討之資安技術研析為 Cobalt Strike 後門程式/中繼站調查分析，綜觀 109 年政府機關資安事件，發現駭客常使用 Cobalt Strike 做為攻擊工具。Cobalt Strike 是用於模擬紅隊演練之主從式架構滲透測試軟體，協助組織進行團隊協作與入侵攻擊演練。

近年常發現 Cobalt Strike 被用於各種 APT 攻擊行動，如 APT19, APT29, APT32, APT41, Cobalt Group, Chimera 等，再加上 Cobalt Strike v4.0 原始碼據稱已於 109 年外洩於 GitHub 原始碼平台，駭客利用 Cobalt Strike 進行駭侵活動恐再加劇。相關常見攻擊活動中，駭客除透過社交工程惡意電子郵件散布後門程式(Beacon)，亦使用 HTTP(S)或 DNS 隧道通訊(DNS Tunnel)等加密技術，偽冒合法網站隱藏中繼站(Team Server)連線資訊，進行資料竊取。

3.1 情蒐分析與研究調查流程

109 年透過惡意電郵偵測機制，發現 3 波使用 Cobalt Strike 後門程式之 APT 攻擊行動，以社交工程惡意電郵鎖定特定機關進行入侵行動。透過網路威脅情蒐，109 至 110 年分析政府機關受駭報到行為紀錄，主要可分成 DNS 隧道通訊與 HTTP 連線回報。

技服中心依相關威脅情蒐資訊，規劃 Cobalt Strike 後門程式之情蒐分析與研究調查流程，詳見圖 9。



資料來源：本報告整理

圖9　Cobalt Strike 後門程式之情蒐分析與研究調查流程

首先進行工具研究與樣本分析，Cobalt Strike 網路架構為主從式架構，C&C 伺服器以 Team Server 為中繼站本體，支援多個攻擊者同時連線，主要擔任與受駭主機端通訊之伺服器主機。Beacon 為攻擊者所產生之後門程式，感染受駭主機後，負責與中繼站進行溝通。Listener 功能為負責後門程式與中繼站溝通之通訊協定，攻擊者指定 Listener 後方能產製對應之惡意程式。Client 程式則提供 GUI 予攻擊者連線至 Team Server 操作控制受駭主機，包含取得螢幕截圖、列舉系統執行程序及竊取使用者帳密等攻擊行為。此外，Cobalt Strike 還提供客製化配置文件(Malleable C2 Profiles)予攻擊端設定，藉此改變通訊傳輸特徵規避流量檢測。

第 2 個步驟為惡意程式樣本蒐集，經分析 Beacon 後門程式，針對其加解密等特徵撰寫 YARA 偵測規則，部署至 VirusTotal 情資平台，進行樣本狩獵，蒐集 109 年 9 至 11 月之 Cobalt Strike 後門程式(Beacon)，幾近 3000 隻樣本。

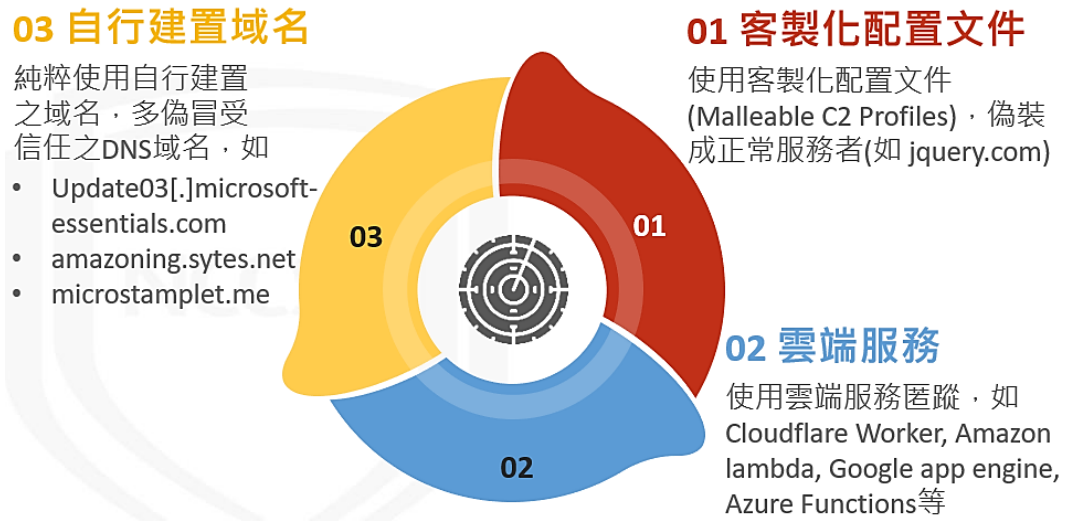
第 3 個步驟為樣本配置檔萃取，Cobalt Strike Beacon 後門程式含有駭客設

定配置檔(Profile)之資訊，經解密與對照後可得到明文之設定資訊，調查針對所蒐集之樣本，逐一萃取配置檔資料進行統計分析。

第 4 個步驟為配置檔情蒐分析，本次所發現之 Cobalt Strike Beacon 後門程式以版本 3 占 83%為最多，惟版本 4 已於 108 年 12 月釋出，並於 109 年 3 月陸續出現未完全破解版本，直至 109 年 11 月發生版本 4 原始碼外洩，預期未來使用版本 4 之後門程式數量將大幅增加。此外，分析 Cobalt Strike 後門程式使用之通訊協定，以 DNS 為最多(占 77%)；分析使用之通訊埠號，以 HTTPS(443)為主(占 87.16%)。調查亦發現駭客使用 Amazon 模板為最多，其次為 Cobalt Strike 預設模板，其他常被使用之模板包含 Webbug、jQuery 及 OCSP。

第 5 個步驟為全球中繼站掃描，整合蒐集樣本中繼站與透過開源威脅情資(Open Source Intelligence, OSINT)，蒐集篩選威脅性高之攻擊來源做為掃描清單列表，利用 NMAP 工具進行掃描，辨識可疑之中繼站伺服器。

最後一個步驟為中繼站分析，針對 Cobalt Strike 中繼站進行特徵樣態分析，辨識蒐集全球中繼站伺服器資訊。經剖析中繼站掃描結果樣態，Cobalt Strike 連線中繼站匿蹤技術可分為 3 種樣態，詳見圖 10。

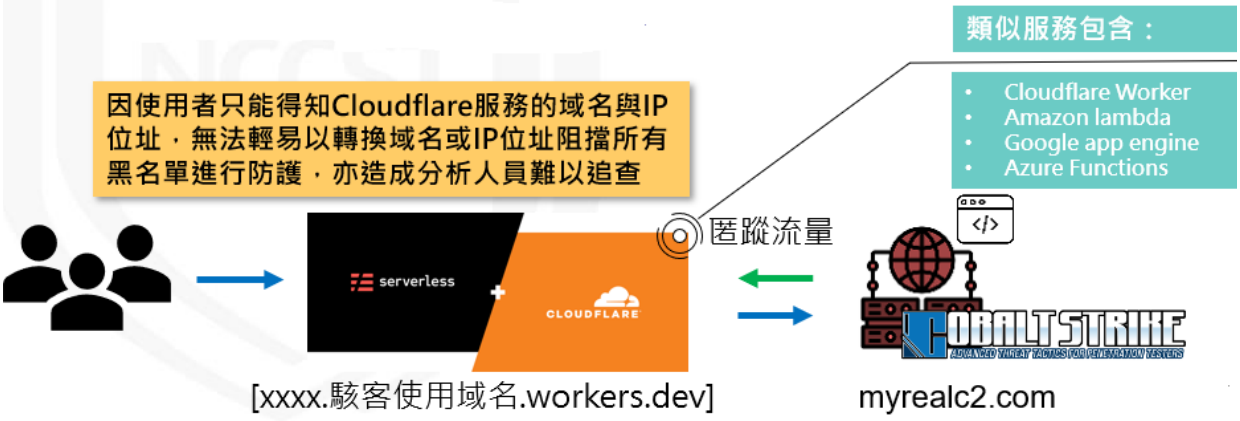


資料來源：本報告整理

圖10 Cobalt Strike 連線中繼站匿蹤技術之 3 種樣態

3.2 Cobalt Strike 連線中繼站後續追蹤與監控

經掃描分析發現，Cobalt Strike 伺服器有逐步朝向部署於雲端平台之趨勢，推測駭客租用雲端服務平台之 IP 位址，藉此規避資安防護阻擋機制，並隱匿駭客行蹤。攻擊者以內容傳遞網路(Content Delivery Network, CDN)做為網路服務前端，匿蹤實際 C2 域名與 IP 位址，以 Cloudflare 之 Worker 服務為例，若註冊名為 microsoftupdate 之 Worker，駭客同時可得到該子域名為 microsoftupdate.workers.dev。當受駭電腦連線前述可疑域名，將透過 Cloudflare 服務經多階段域名轉換，最終才得到中繼站之回應，惟匿蹤轉換之域名與實際伺服器 IP 位址皆無跡可尋，詳見圖 11。



資料來源：本報告整理

圖11 偽冒 DC 身分與 DC 建立安全通道

在技服中心持續追蹤下，於 109 年 12 月偵測發現某機關有受駭連線 Cobalt Strike 中繼站之行為，經發布警訊後比對情蒐分析取得之惡意中繼站 IP 位址與偽冒域名，可回溯該機關更早受駭日期，並監測發現該機關遭持續擴大入侵之相關連線跡證。

針對 Cobalt Strike 攻擊與連線回報等惡意連線行為，技服中心持續開發相關偵測機制並監控惡意連線行為，如 DNS 隧道通訊回報，透過開發 DNS 異常偵測演算法，由每日 DNS 日誌萃取異常指標分析，成功偵測政府機

關受駭案例；HTTP(S)連線回報，因多為加密連線，過往不易偵測，將透過網路公開樣本、社交工程攻擊及網路威脅情資蒐集，再整合 Cobalt Strike 可疑中繼站掃描驗證，確認相關威脅指標之回報樣態，共計取得多個惡意中繼站 IP 位址與偽冒域名。

時至今日，Cobalt Strike 已成為駭侵組織常用之攻擊工具，因具有資訊隱藏、傳輸加密機制及偽裝模板特徵配置，可躲避網路偵查，同時亦造成情蒐分析人員難以分辨背後之真實駭侵組織。藉由訂定研究分析流程，擴大研析 Cobalt Strike 惡意程式與情蒐全球中繼站伺服器，取得惡意程式、惡意中繼站 IP 位址及偽冒域名。接續將再透過發展 DNS 異常行為偵測機制與結合骨幹回溯機制，持續偵測受駭機關，並進行即時告警。另外，相關入侵指標(Indicator of Compromise, IoC)情資已透過聯防監控月報提供國內相關單位進行聯防，未來亦規劃透過國家資安資訊分享與分析中心(N-ISAC)分享研析報告予國內外資安組織，進行經驗交流。

4. 結論

本季具指標性案例為探討美國淨水處理廠遭不明駭客入侵，試圖調高水中氫氧化鈉濃度事件，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 TeamViewer、未安裝防火牆防護及共用密碼等不安全使用行為，關鍵基礎設施之影響範圍重大且深遠，資通安全防護技術應全面檢視與提升。第 2 起案例為為資安業者揭露 NoxPlayer 供應鏈攻擊行動，駭客透過 NoxPlayer 更新機制，於用戶執行更新時植入惡意程式，該惡意程式主要用途為蒐集用戶鍵盤輸入紀錄與機敏資訊等，資通系統更新前應做好驗證與測試動作，即時偵測任何異常行為。

國內部分，分析政府資安威脅現況，發現政府機關通報事件類型，以「非法入侵」為主，綜合類型「其他」次之，接續分別為「設備問題」與「網頁攻擊」。針對本季全球與政府所面臨之主要資安威脅，本報告就「關鍵資訊基礎設施資安管理」與「系統自動更新之資安管理」及「隨身碟之資安管理」，提出資安防護建議。

資安專題分享主題為零信任網路設備鑑別簡介，概述設備之鑑別與健康管理之零信任網路技術。同時以開源軟體為主，於零信任網路中規劃設備鑑別架構並進行 PoC，包含建置設備代理器(設備鑑別與健康管理)、設備健康管理伺服器及設備鑑別伺服器，以驗證與完備零信任網路資安環境。

另外，資安技術研析主題為 Cobalt Strike 後門程式/中繼站調查分析，109 年透過惡意電郵偵測機制，發現 Cobalt Strike 後門程式之 APT 攻擊行動。針對 Cobalt Strike 攻擊與連線回報等惡意連線行為，開發相關偵測機制並監控惡意連線行為，藉由訂定研究分析流程，擴大研析 Cobalt Strike 惡意程式與進行中繼站伺服器情蒐。