111年第3季資通安全技術報告

Quarterly Technical Report

目　次

圖 目 次

摘要

「第 3 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 3 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 起案例為社群媒體遭駭或利用，成為駭客謀利工具；另一起案例為勒索軟體族群運用新式間歇性加密技術，快速加密受駭者系統。

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 45.84%)類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」(占 10.83%)與「設備問題」(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滲透測試輔助技術研析，人工滲透測試由於人力資源限制，無法大規模與經常性執行滲透測試專案，且人工判斷致缺乏評估系統漏洞之廣度與完整性。自動化滲透測試可藉由工具，採步驟式完成情蒐、弱掃及漏洞驗證等項目，揭露與驗證各種潛在漏洞，分析各種攻擊步驟，以提升測試能量。

●3.資安技術研析

資安技術研析主題為 BlackTech 族群追蹤與樣態分析，發現進階持續性威脅攻擊活動持續有增長趨勢，於外部 APT 相關情資亦觀察到該族群相關活動，顯現 BlackTech 族群鎖定特定政府機關之攻擊再起。

●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。資安專題分享滲透測試輔助技術研析，研析運用人工智慧所發展之滲透測試自動化輔助技術，針對內網滲透測試之目標環境產出攻擊路徑與方法，期藉此提升滲透測試之攻擊效率。此外，資安技術研析分析 BlackTech 族群追蹤與樣態，發現攻擊策略以 APT 攻擊為主軸，揭露駭客近年來對部分程式進行邏輯調整，目的為加強隱蔽性，避免被快速偵測。

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 3 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

隨著數位轉型，資安升級也勢在必行，在全球與國內因特殊政經因素情況下，造成資安情勢越趨緊張，政府與民間更需強化公私協力及國際合作交流。除持續關注全球資安威脅變化狀況外，更可藉由與國際夥伴合作、交流情資，讓資安防護網路更加嚴密且精進。

本季全球資安威脅聚焦在討論社群媒體普及化之情況，如何確保官方或具代表性之社群媒體帳號相關安全性。同時，隨著駭客運用新興技術入侵，且藉由勒索軟體即服務之便利性大舉入侵時，機關應如何全面加強資安防護策略。

本季具指標性案例為社群媒體遭駭或利用，成為駭客謀利工具；另一起案例為勒索軟體族群藉由新式間歇性加密(Intermittent Encryption)技術，快速加密受駭者系統。

首先，探討案例為社群媒體帳號遭入侵後，駭客藉此竊取資訊與謀取利益。時至今日，各國政府機關官網常有遭駭情形發生，惟現在駭客將目標擴大至社群媒體，英國陸軍推特帳戶及 YouTube 頻道分別擁有逾 36 萬名粉絲與 18 萬人訂閱，近期同時遭駭客入侵，其推特頁面遭竄改成 The Possessed NFT Project 之頁面，並於推文中假借 NFT 行銷活動之名，夾帶

惡意連結；Youtube 頻道則遭更換為由 Cathie Wood 創立之方舟投資 ARK Investment Management 頁面，並循環播放以特斯拉創辦人 Elon Reeve Musk 與推特聯合創始人 Jack Patrick Dorsey 舊影片改製之假宣傳影片，宣稱可協助使用者將比特幣與乙太幣翻倍。

類似事件為近期發現駭客利用 YouTube 假借遊戲教學或破解攻略影片，卻於影片中夾帶惡意軟體套件組，遭假借之知名遊戲包含 FIFA, Final Fantasy, Forza Horizon, Lego Star Wars 及 Spider-Man 等。

資安廠商 Kaspersky 報告指出，在 RAR 壓縮檔中內隱藏一系列惡意軟體，最知名為一款稱為 RedLine，是目前散播最為廣泛之資訊竊取軟體。使用者一旦安裝，RedLine 會竊取受駭者網路瀏覽之相關資訊，包含 cookie、帳戶密碼、信用卡資訊、即時通訊內容及破解加密貨幣錢包。此外，該壓縮檔內尚暗藏挖礦程式，駭客更可利用受駭者之系統資源挖礦，藉此獲得更多利益。同時，因為在此惡意軟體套件組中，有一合法之 Nirsoft NirCmd 公用程式，可以在不啓動任何視窗下執行動作，因此更讓使用者難以發現其蹤跡。

第 2 起案例為勒索軟體族群採用新式間歇性加密(Intermittent Encryption)技術，以快速加密受駭者系統，同時減少被偵測機率。間歇性加密不同以往勒索軟體加密法，只加密目標文件之部分檔案內容，以加速受駭者系統之加密速度。因其只加密部分內容，所以加密過程幾乎只需完全加密一半時間，且若不使用有效之解密方法與密鑰，仍無法使資料回復，依據此加密方式，將使過往偵測工具慣用檢測方式，包含統計分析文件 IO 運作強度評估或版本差異性比對，無法有效且即時偵測異常狀況。

美國資安廠商 SentinelLabs 指出，採用間歇性加密已成勒索軟體之最新趨勢，LockFile 為第一個使用間歇性加密之勒索軟體，依每 16 位元組之間隔執行加密。由於間歇性加密技術相對容易建置，因此越來越多勒索軟體包

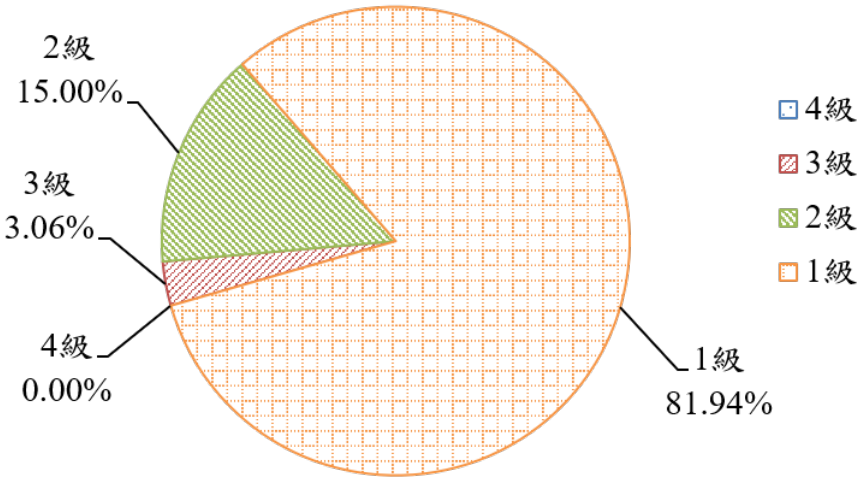
含 Qyick、Agenda、BlackCat (ALPHV)、PLAY 及 Black Basta 採用此手法。

採用間歇性加密之勒索軟體已發展出勒索軟體即服務(Ransomware-As-A-Service)，早在去年暗網就出現第一個以 Rust 語言編寫之勒索軟體 BlackCat (ALPHV)。SentinelLabs 於本年 8 月時亦觀察到有使用者在暗網販售 Qyick 勒索軟體，採一次性購買，而非常見之訂閱模式，同時保證若該勒索軟體於購買後 6 個月內被偵測工具檢測出，將獲得一個新樣本，且提供折扣價。間歇性加密因具備可快速加密檔案、能規避資安工具偵測且建置容易，因此 SentinelLabs 之分析師預測將有更多勒索軟體使用此方式加密資料。

綜覽本季重大資安事件，駭客將目標擴大至社群媒體，社群媒體因使用者廣泛，資安意識參差不齊，致駭客利用竄改之頁面進行詐騙行銷或假借遊戲教學與破解攻略影片，夾帶惡意軟體套件組，造成使用社群媒體群眾防不勝防。隨著勒索軟體攻擊盛行，不僅發展出新式間歇性加密技術，更因勒索軟體即服務在暗網唾手可行，造成此類攻擊在全球與國內之資安事件屢見不鮮。

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 81.94%為大宗，2 級事件占 15%次之，3 級事件僅占 3.06%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

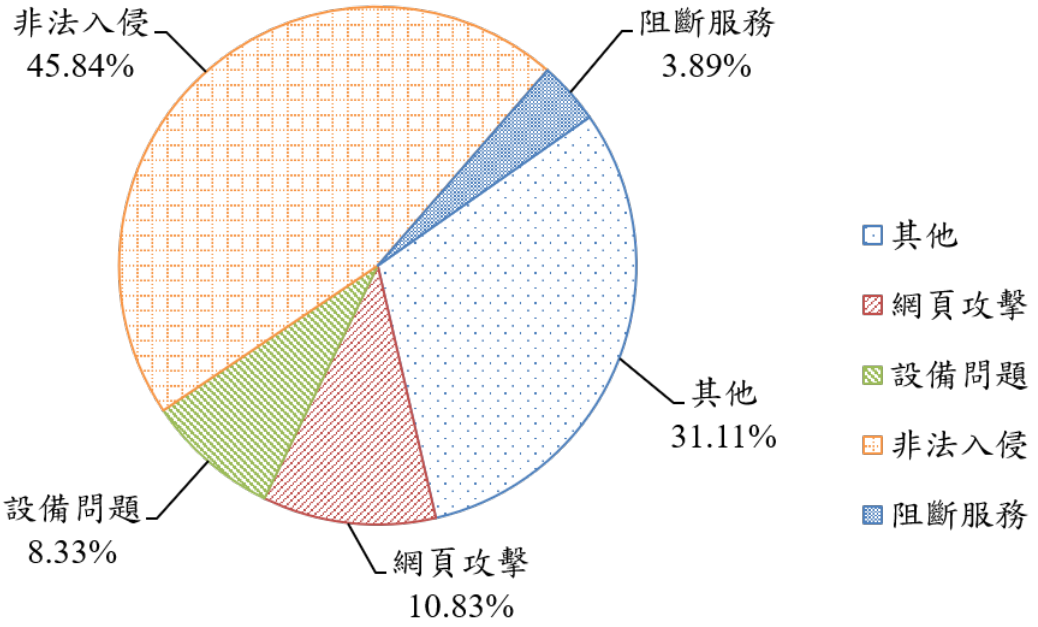


資料來源：本報告整理

圖1　111 年第 3 季通報事件影響等級比率圖

本季接獲之重要通報事件，發生個人電腦遭勒索軟體加密事件，調查後發現入侵原因為使用者瀏覽網站時，點擊下載偽冒成微軟更新檔之程式，導致受駭。陸續仍發現部分機關電子看板或網站顯示之資訊遭惡意置換，調查後發現系統雖使用 SSH(Secure Shell)加密連線，惟管理帳號使用弱密碼致遭暴力破解。

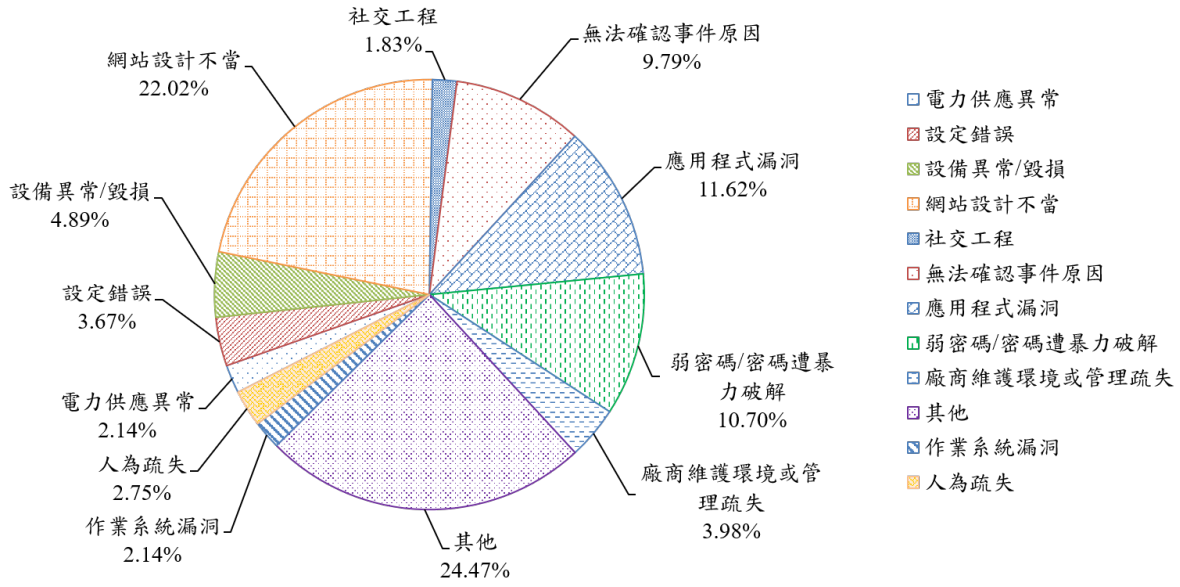
整體事件比率，以「非法入侵」(占 45.84%)類型為主，排除綜合類型「其他」外，「網頁攻擊」與「設備問題」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　111 年第 3 季通報類型比率圖

最後，分析通報事件發生原因，可發現事件原因以其他(24.47%)與網站設計不當(22.02 %)為主要原因，其次分別為應用程式漏洞(11.62%)、弱密碼/密碼遭暴力破解(10.7%)、無法確認事件原因(9.79 %)、設備異常/毀損(4.89%)、廠商維護環境或管理疏失(3.98%)、設定錯誤(3.67%)、人為疏失(2.75%)、電力供應異常(2.14%)、作業系統漏洞(2.14%)及社交工程(1.83%)，詳見圖 3。本季無法確認事件原因之比率為 9.79%，相較於上季之 20.98%，比率明顯下降，可見資通安全管理法推動之事件日誌與可歸責性漸具成效，機關已就資通系統防護基準要求之日誌記錄時間訂定週期及留存政策，並保留日誌至少六個月，同時確保資通系統具備記錄特定事件之功能，如此一來，對資安事件追查大有助益。



資料來源：本報告整理

圖3　111 年第 3 季通報事件發生原因比率圖

分析第 3 季通報事件發生原因，有部分為實兵演練所揭露之通報事件，部分機關網站因使用第三方應用程式套件 CKEditor 與 CKFinder，惟其套件版本過舊存在弱點，被跨站腳本攻擊成功，或因檔案上傳功能未限制存取遭利用，被成功上傳實兵演練圖檔。弱密碼部分發現仍有機關以常見鍵盤位置排序(如 1qaz@WSX)設置郵件密碼，雖符合密碼設定安全性原則，惟已列入駭客常見之暴力破解清單，應特別注意此類密碼設定方式。

1.3 資安防護重點

分析本季全球資安威脅現況，駭客已擴大其入侵目標至官方社群媒體，藉由其眾多流量與訂閱使用者，實施行銷詐騙行為與夾帶惡意程式以竊取機敏資料。另一個可預見之威脅為駭客使用新興技術使其攻擊行為更加隱匿與快速，因此資安防護技術亦應持續精進，以防範相關攻擊。

國內部分發現弱密碼攻擊事件，需要特別加以宣導之密碼設定原則，並非符合安全性設定原則即可，部分以常見鍵盤位置排序設定之密碼仍應視為

弱密碼。現組態設定原則雖採取系統化檢視，應定期檢視組態設定之安全性；規劃系統管理者或使用者之資安專業訓練，年度採取滾動式檢討，就常見之威脅與相對應風險提出應對方案，避免人員因便宜行事而淪為資安破口。

綜整以上資安威脅現況，提供資安防護建議如下：

●防範勒索軟體採間歇性加密之資安管理

– 訂定完善之定期備份管理政策，並須包含一份離線副本。

– 採用精進縱深防禦之資安防禦架構，如強化反釣魚(Anti-phishing)能量，包含人工智慧偵測機測、WAF(Web application firewalls)防火牆及延伸偵測及回應(Extended Detection and Response, XDR)等機制。

– 針對新與科技或技術之可能威脅制定使用者訓練計畫，強化使用者事件認知與因應等意識。

●SSH 連線之資安管理

– 針對 SSH 連線進行組態安全設定檢視，修改預設登入方式與連線方式，如新增另一個擁有管理者權限帳號，並設定符合安全性原則之密碼。

– 限制登入失敗次數，且定義超過一定錯誤次數後必須等待特定時間後才能再次登入。

– 定期於防火牆設置與維護白名單，限制 IP 範圍之電腦方能連線。

2. 資安專題分享_滲透測試輔助技術研析

滲透測試服務通常需要較多人力投入，過程中需要專家模擬駭客攻擊，運用多種攻擊技術、手法，以確認目標系統之防護程度，同時需提出精準之評估報告，並提供改善建議策略與方向。解析滲透測試每個階段，從第一步驟資料蒐集相關網路與系統資訊，如域名、開啓之連接埠、軟體、硬體、韌體及帳號權限等；第二步驟以弱點掃描方式進行漏洞蒐集；接續第三步驟進行漏洞探索，建立並分析攻擊路徑規劃；第四步驟則為進行目標系統之漏洞驗證，包含內部驗證滲透程序、對受測系統展開攻擊，成功進入後展開提權或橫向攻擊活動；最後步驟則仰賴專家分析所有流程後，進行報告撰寫，說明攻擊過程與揭露之系統或其他漏洞，並提供修補建議。

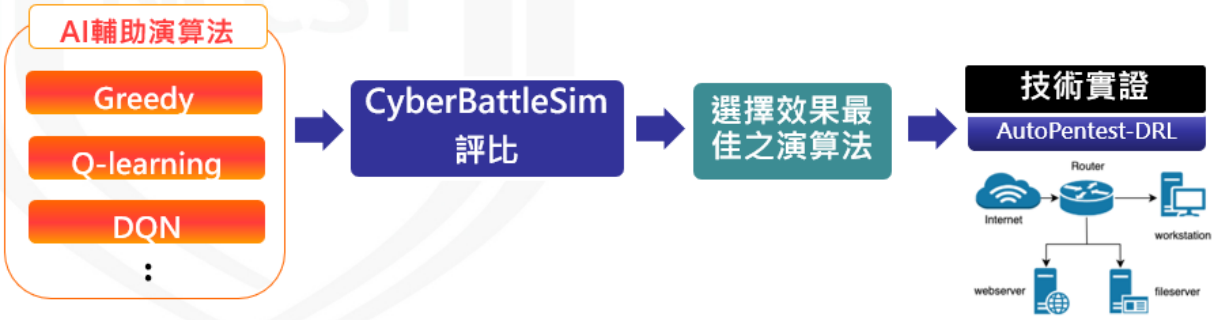
面對人工密集要求之滲透測試流程與駭客攻擊之多樣態，為提升滲透測試服務之檢測品質與效率，本報告研析運用人工智慧所發展之滲透測試自動化輔助技術，針對內網滲透測試之目標環境產出攻擊路徑與方法，做為攻擊策略之參考，期藉此提升滲透測試之攻擊效率。

2.1 滲透測試輔助技術探討

人工滲透測試囿於專家團隊人力有限情況下，無法大規模與經常性執行滲透測試專案，同時因為依賴人工判斷，恐因個人偏好或經驗限制搜尋特定領域，缺乏評估系統漏洞之廣度與完整性。自動化滲透測試可藉由工具採步驟式完成情蒐、弱掃及漏洞驗證等項目，揭露與驗證各種潛在漏洞，分析各種攻擊步驟，大規模提升測試能量，在效率與測試規模考量下，亦應積極研析自動化滲透測試輔助技術與實證。

技服中心首先設定之研究目標為綜整以人工智慧(Artificial Intelligence, AI)輔助滲透測試之相關研究，主要用於輔助產生較佳攻擊路徑，以縮減滲透測試人員探索時間。研究策略則針對可產生攻擊路徑之 AI 輔助演算法，運用由微軟所發展之模擬分析平台 CyberBattleSim 進行評比，選出效果最

佳之演算法，再針對該演算法進行下階段之技術實證，詳見圖 4。



資料來源：本報告整理

圖4　自動化滲透測試輔助技術研討與實證流程

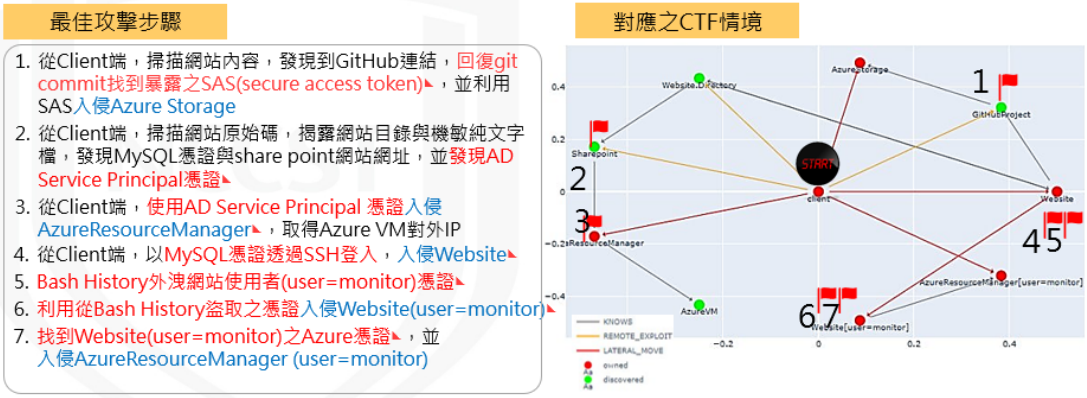
CyberBattleSim 為微軟開發之 AI 模擬研究工具，採用智慧型代理人(Agent)技術，模擬內部網路遭入侵後(Post-breach)，攻擊者進行弱點利用與內網橫向移動過程。微軟釋出內部 AI 模擬研究工具之 Python 原始碼，目的為模擬攻擊者入侵網路後之動作，包含執行本機攻擊、遠端攻擊及連結其他節點等 3 種攻擊行為，藉由模擬攻擊活動，評比 AI 輔助演算法之攻擊效率，提供資安人員後續參考與運用。

CyberBattleSim 提供由 Python 原始碼撰寫之 OpenAI Gym 介面，用於增強式學習演算法訓練智慧型代理人(Agent)程式。OpenAI Gym 來自 Elon Musk 所創立之非營利人工智慧研究公司(OpenAI)，常見應用於開發、訓練及評估增強式學習演算法之測試互動環境，如開發電玩、機器人模擬及控制系統等用途。

此次滲透測試輔助技術探討，首先設定 CyberBattleSim 之測試情境以奪旗(Capture The Flag, CTF)方式呈現，並由客戶使用者 Client 端為起點進行攻擊。準備含有 10 台主機之內網環境，內含 7 個可由滲透測試取得之旗幟(Flags)。

從測試情境中可得知，攻擊擴散具有順序關係，不同順序將導致測試分數

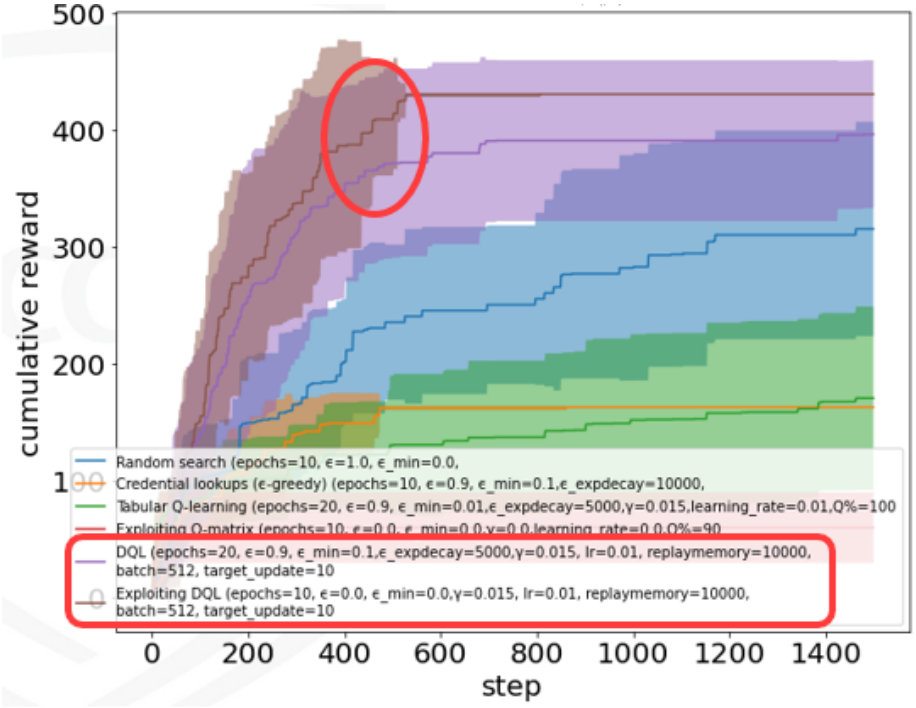
差異。若要取得最佳獎勵(Reward)分數，必須以最佳攻擊步驟進行擴散攻擊，規劃出正確依序進行掃描、獲取資訊及揭露憑證訊息，並順利入侵主機取得控制權，從測試環境中，模擬出之最佳攻擊步驟，詳見圖 5。



資料來源：本報告整理

圖5　CyberBattleSim 測試情境中之最佳攻擊步驟

CyberBattleSim 之結果分析，可以從微軟報告(https://www.microsoft.com/security/blog/2021/04/08/gamifying-machine-learning-for-stronger-security-and-ai-models)中得知，比較 AI 輔助、隨機代理人及真人操作之攻擊成效，AI 輔助法所耗費步數最少，應用 AI 可有效提高攻擊效率，測試案例則顯示 AI 輔助智慧型代理人(Agent)約花 20 步取得所有控制權，隨機代理人約花 500 步取得所有控制權，專家人工作業平均約花 50 步取得所有控制權。根據演算法成效圖顯示，深度增強式學習模型(Deep Q-learning, DQN)效率最佳，可以最少步數取得最高分數，詳見圖 6。



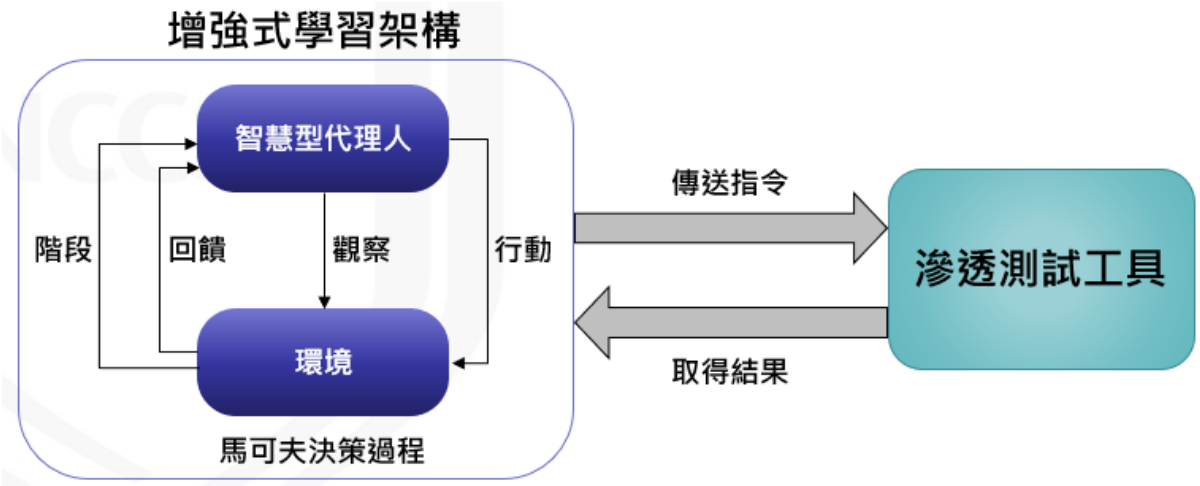
資料來源：本報告整理

圖6　演算法成效分析

依據此次比較結果，以下將採用相關 DQN 工具進行技術實證。

2.2 滲透測試輔助技術實證

滲透測試輔助技術實證採用增強式學習(Reinforcement Learning)推演攻擊手法，著眼於演練環境設計，透過過每一次錯誤學習，以取得最佳之攻擊路徑。馬可夫決策過程(Markov Decision Process, MDP)用於建構滲透測試模擬訓練環境，透過訓練智慧型代理人，可依據環境狀態分析出建議之攻擊動作。每當應用到新的測試環境時，增強式學習模型皆須重新訓練，訓練結果產出即為最佳之執行策略，詳見圖 7。

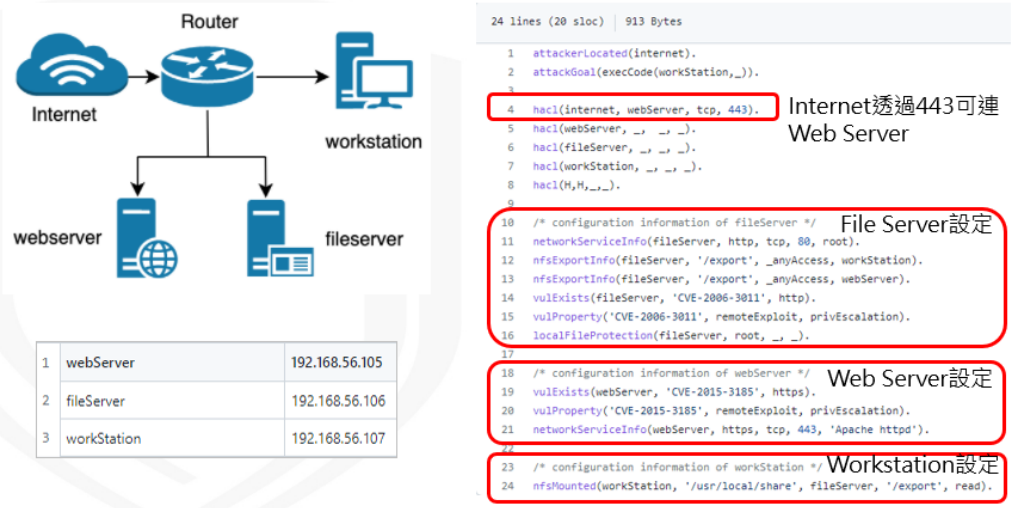


資料來源：本報告整理

圖7　增強式學習推演攻擊手法

滲透測試輔助技術實證採用 AutoPentest-DRL 自動化滲透測試架構，此為基於 DQN 演算法之自動化滲透測試架構，主要用於內網滲透測試，可對測試目標進行情蒐，產生攻擊樹與轉移矩陣，接著利用深度增強學習模型，分析出最佳攻擊路徑，再運用滲透測試工具 Metasploit 對目標網路執行模擬攻擊。

AutoPentest-DRL 測試情境設定於 Workstation 執行攻擊程式，模擬情境當攻擊者利用 Web Server 具權限提升或可執行任意程式碼之漏洞，藉由 File Server 之網路檔案系統(Network File System, NFS)服務安裝木馬程式，利用其分享檔案之特性植入木馬於 Workstation。模擬環境包含 1 台 Web Server、1 台 File Server 及 1 台 Workstation，相關網路環境拓樸設定檔，詳見圖 8。



資料來源：本報告整理

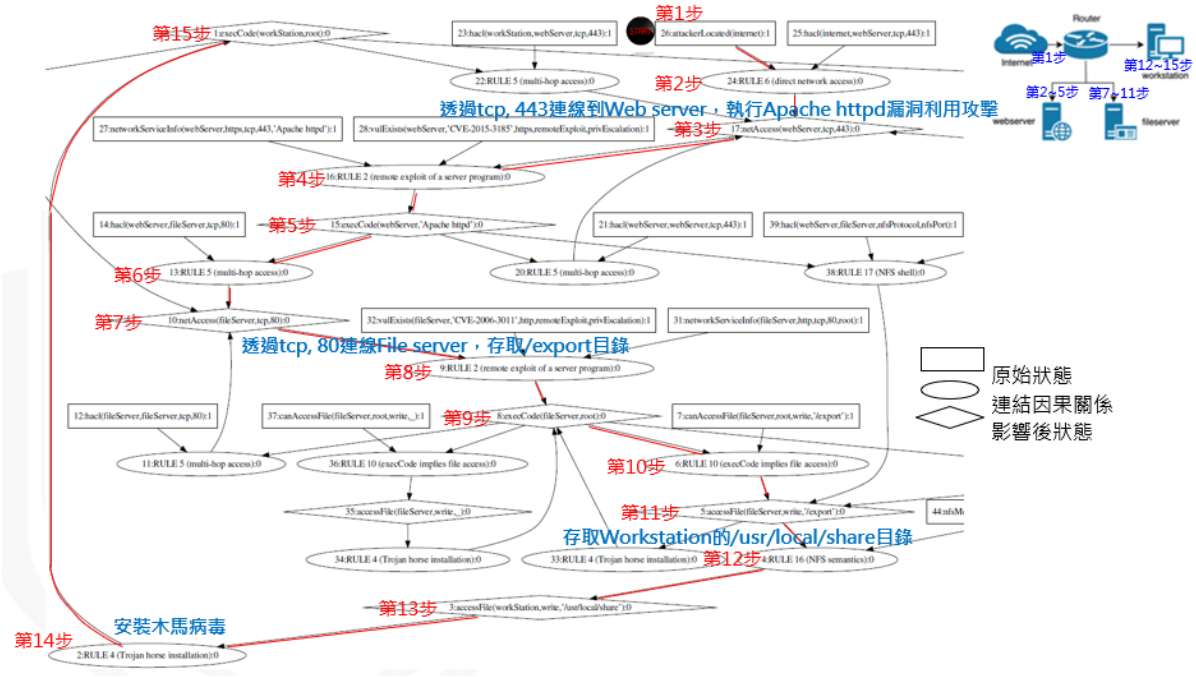
圖8　網路環境拓樸設定檔

AutoPentest-DRL 之測試結果包含攻擊圖，藉由連結各個主機已知之漏洞，模擬攻擊者可行之所有路徑，詳見圖 9。

資料來源：本報告整理

圖9　工具輸出攻擊結果

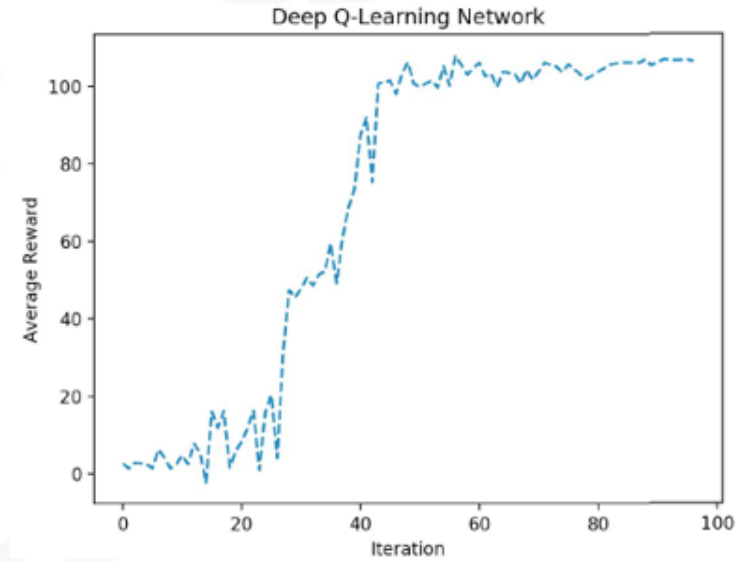
攻擊圖上以紅色標記最佳攻擊路徑，從其路徑得知攻擊者從 Internet，透過 tcp 443 連線到 Web server，利用 Web server 具權限提升或可執行任意程式碼之漏洞，執行 Apache httpd 漏洞利用，再利用 File server 其分享檔案之特性，建立/export 目錄，存取 Work Station 之/usr/local/share 目錄，最終以 Workstation Root 權限成功執行木馬程式，詳見圖 10。



資料來源：本報告整理

圖10 模擬出最佳攻擊路徑

從此次測試環境模型訓練之累計分數變化圖中，觀測深度增強學習模型(DQN)在模型訓練 100 代之獎勵(Reward)分數變化，一開始呈現緩慢成長，從第 30 代左右開始大幅成長，至第 40 代後逐漸成長趨緩，惟亦表示已發現最佳攻擊路徑，詳見圖 11。



模型訓練之累計分數變化圖

最佳攻擊路徑標記紅色

資料來源：本報告整理

圖11 模型訓練之累計分數變化

技服中心研究團隊此次規劃測試場域，以實證研析滲透測試輔助技術，運用模擬分析平台 CyberBattleSim 進行評比，驗證增強式學習之 AI 技術具備較佳攻擊路徑探索能力。此外，亦進一步針對深度增強式學習開源工具 AutoPentest-DRL 進行測試，於內網滲透測試之實驗場域環境驗證其可行性，並進行演算法成效分析。後續研究重點將持續關注滲透測試輔助技術發展，研析與應用相關開源工具，並持續探討於不同應用情境下所適用之滲透測試輔助技術，以分析更精準之攻擊手法，輔助執行滲透攻擊與研擬緩解建議。

3.資安技術研析_BlackTech 族群追蹤與樣態分析

本季探討之資安技術研析為 BlackTech 族群追蹤與樣態分析，技服中心藉由觀測部署於政府網際服務網(Government Service Network, GSN)骨幹之入侵防禦系統(Intrusion Prevention System, IPS)所蒐集之情資，發現 111 年第 2 季開始，進階持續性威脅(Advanced Persistent Threat, APT)攻擊活動持續有增長趨勢，其中尤以 BlackTech 族群最為顯著。

分析上半年事件，主要以 WaterBear 惡意程式之駭侵活動案件為主，部分事件中更偵測到許久未曾出現之樣本特徵。同時，於外部 APT 相關情資亦觀察到該族群相關活動，顯現 BlackTech 族群鎖定特定政府機關之攻擊再起。

3.1 BlackTech 惡意程式概述與事件案例

分析 111 年 BlackTech 族群相關案件，自 108 年起 WaterBear 案件比例有逐年增加趨勢，攻擊策略以 APT 攻擊為主軸，由其惡意程式樣本分析，可以看出駭客近年來對部分程式進行邏輯調整，以加強隱蔽性，避免被快速偵測。

從近期資安事件所搜查之惡意中繼站分析，惡意程式以 WaterBear 分支為主，持續追蹤觀察中繼站活動，發現與去年調研之中繼站狀況相同，以攻擊機關網通設備、無線路由器做為中繼站，案例多發現某型號之無線路由器遭駭客破解登入，並透過 VPN 功能持續操控做為中繼站使用，接收受駭單位報到。檢視該中繼站網路流量，發現有少數政府機關、財團法人及民間企業報到現象。

分析 111 年事件相關 WaterBear 樣本，整體運作模式均與過往樣本有所重疊，從已掌握之樣本行為鍊(Behavior Chain)得知，惡意程式啓動方式在近期案例中最盛行以正常程式載入，可藉此隱匿蹤跡，再透過 ShellCode 載

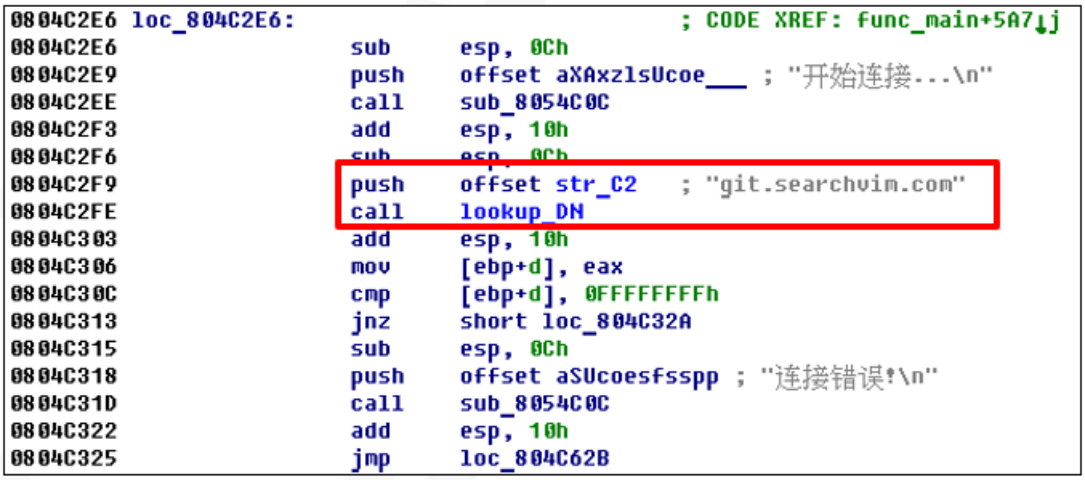
入方式，讀取外部檔案或 Registry。進一步分析 ShellCode，其功能類型分別為主動報到型、被動控制型、木馬側錄型及運作干擾型，主要流量特徵則有明文傳送及編碼加密等類型。

以下將針事件案例進行彙整與樣本研究，進行更深入之關聯分析。

3.2 惡意程式樣本關聯分析

首起事件之樣本，為該族群駭客針對 Unix/Linux 平台所開發之後門程式 Biforse，此族群亦持續更新該類型惡意程式。駭客團體曾利用此程式入侵政府機關、政府委外廠商及民間企業，如醫療、金融及電子產業等。技服中心所發現之事件案例為某機關因產生異常流量，致觸發偵測規則，透過 HTTP Protocol 存取網路資源之協定 Curl 所下載之程式，即為 ELF 惡意程式 Biforse。

經調查此機關遭駭主因為 F5 負載平衡器漏洞(CVE-2022-1388)遭利用，允許入侵者可繞過 iControl REST 元件之身分鑑別程序，進而存取 F5 BIG-IP 系統，並遠端執行任意程式碼。進一步分析此 Biforse 樣本，發現其最早可追溯至 2004 年，BlackTech 族群將原始版本調整後使用之後門程式，其原始版本 registry 欄位：HKLM\SOFTWARE\Bifrost\nck HKCU\Software\Bifrost\klg，修改版本為 registry 欄位：HKLM\SOFTWARE\NKav\nck HKCU\Software\NKav\klg。該樣本透過讀取設定檔內中繼站 DN(git.searchvim[.]com)並查詢對應 IP，中繼站領域名稱(Domain Name, DN)則為明文顯示，連線訊息顯示字型為簡體中文，詳見圖 12。



資料來源：本報告整理

圖12 惡意中繼站 DN

進一步與外部情資樣本比較，發現運作功能與 RC4 key 均相同，差別為是否經過最後的查表加密步驟，詳見圖 13。

來源	外部情資(2020)	本案樣本1	本案樣本2
MD5	3319b4dbe54e8dc49176b628a266b240	ea34dfd801cc5ed833a2c3ec282dba39	4a443aab638ec88a8a6439e6b25907d0
類型	Compiler : GCC: (GNU) 4.1.2 20071124 (Red Hat 4.1.2-42)	Compiler : GCC: (GNU) 3.2.3 20030502 (Red Hat Linux 3.2.3-42)	Compiler : GCC: (GNU) 3.2.3 20030502 (Red Hat Linux 3.2.3-42)
版本號	5.0.0.0	5.0.0.0	5.0.0.0
大小	574,140 bytes	453,124 bytes	486,020 bytes
RC4加密	是	是	是
RC4 KEY	A378263557322D60B43C2A5E33347200	A378263557322D60B43C2A5E33347200	A378263557322D60B43C2A5E33347200
查表加密	否	是	是

資料來源：本報告整理

圖13 樣本分析比較

另一事件案例發生在某機關附屬之官網、資料庫及交流平台受駭事件，作業系統皆為 Linux，遭駭主因為利用 PHP 頁面之跨站腳本攻擊(Cross-Site

Scripting, XSS)漏洞入侵，遭植入惡意程式並橫向擴散，受駭主機皆產生異常程序 udevd，惟原後門程式已遭刪除，無法直接取得樣本進行分析程序，推測駭客為躲避鑑識及逆向分析，增加自我刪除功能，於接收結束指令或程序異常結束時，觸發刪除自身程式程序。此事件經流量分析，符合 BlackTech 族群所屬後門程式連線特徵，且持續連線至中繼站報到，惟此事件所觸發之流量特徵，與過往掌握樣本之特徵有些許出入，分析人員無法利用已知 RC4 key 與編碼方式進行解密，僅能以舊版樣本分析與偵測流量進行比對。其中些微差異處，如舊版樣本 Payload 未出現</BODY…>等字，詳見圖 14。

資料來源：本報告整理

圖14 新舊樣本差異處

該樣本功能(HTTP Based Backdoor)入侵首要步驟為蒐集主機資訊(基本負載 Payload)，將主機資訊經變形 RC4 加密、變形 Base64，重新排列編碼，並將加密編碼後之 Payload 放入 HTTP Header 之 Cookie 欄位中。第二步驟則為執行駭客指令，加入額外 Payload，指令包含列舉檔案目錄、列舉程序及列舉磁碟機清單等，將駭客執行結果經變形 RC4 加密、變形 Base64、重新排列編碼，再將加密編碼後之 Payload 放入 HTTP POST Body 中，報

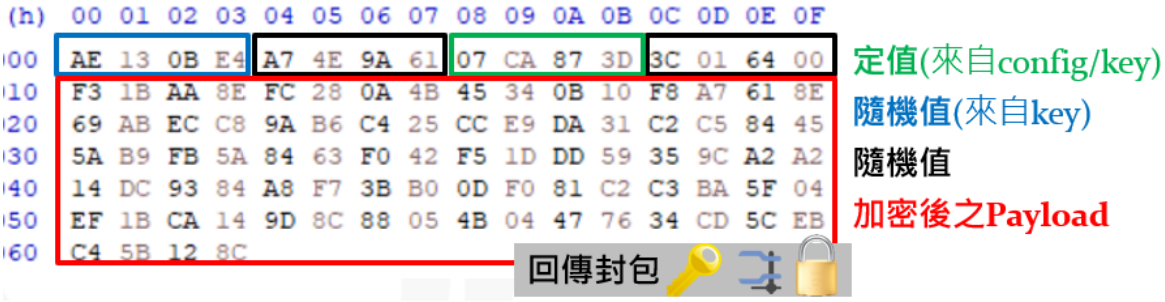
到網路流量詳見圖 15。

資料來源：本報告整理

圖15 駭客增加額外 Payload

另一案件來自於外部情資指出機關遭駭並植入惡意程式，且已成為駭客中繼站。經調查該主機遭植入多種惡意程式，且成為後門程式下載站與中繼站，已逾一段時間並未被發現，而其報到流量將再透過流量轉傳程式將流量導向下一階中繼站，此案件經樣本分析確認惡意程式與 BlackTech 族群中 Plead 類別相關。

樣本分析發現該案之惡意程式執行檔透過 Windows 32bit PE Shellcode Loader 下載執行，第一階段以 RC4 解密自身區段並讀取設定檔執行。第二階段回傳報到封包，Payload(長度 0x13c)為隨機產生並經壓縮，演算法推測為 LZ 變種，加密後之 Payload 詳見圖 16。



資料來源：本報告整理

圖16 加密後之 Payload

分析事件案例發現相關受駭主機除會向惡意中繼站報到外，駭客亦可藉由取得指令或程式供其持續控制。從事件亦知因機關與機關間有資料介接需求，恐將透過資料交換路徑擴大影響其他機關。

因此政府機關除重視委外廠商安全外，亦應關注與評估系統介接時雙方相關資安訊息與風險。另一個發現為駭客有意針對機關網通設備進行攻擊，因此機關應隨時注意設備弱點更新資訊，並即時修補，以防止遭駭客利用擴散。而從存在之駭客工具可知，駭客善於使用隱藏程序與強大蒐集資料功能，因此政府機關應加強威脅偵測時效與回應能力，整合相關資源以強化資安監控能量，充分掌握整體資安狀態，建立主動式偵測與防禦機制。

4. 結論

本季具指標性案例為社群媒體帳號遭入侵後，駭客藉此竊取資訊與謀取利益。舉例英國陸軍推特帳戶及 YouTube 頻道近期同時遭駭客入侵，頁面遭竄改或於推文、影片中假借行銷活動夾帶惡意連結。另一起案例為資安業者指出，採用間歇性加密已成勒索軟體之最新趨勢，由於間歇性加密技術相對容易建置，因此越來越多勒索軟體包含 Qyick、Agenda、BlackCat (ALPHV)、PLAY 及 Black Basta 採用此手法，並發展出勒索軟體即服務。

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「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之主要資安威脅，本報告就「防範勒索軟體採間歇性加密之資安管理」與「SSH 連線之資安管理」提出資安防護建議。

資安專題分享主題為滲透測試輔助技術研析，面對耗費大量人工檢測之滲透測試與多樣態之駭客攻擊，透過研析運用人工智慧所發展之滲透測試自動化輔助技術，針對內網滲透測試之目標環境產出攻擊路徑與方法，提升內網滲透測試服務之檢測品質與效率，以做為攻擊策略之參考。

另外，資安技術研析主題為 BlackTech 族群追蹤與樣態分析，技服中心藉由 GSN 骨幹所蒐集之情資，發現 APT 攻擊活動持續增長，其中以 BlackTech 族群最為活躍。駭客經由攻擊機關網通設備、無線路由器做為中繼站，並透過 VPN 功能持續操控做為中繼站使用，以接收受駭單位報到。從現已掌握之樣本行為錬，發現惡意程式啓動方式以正常程式載入，可藉此隱匿蹤跡，再透過 ShellCode 載入讀取外部檔案或 Registry。

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。

◆ 政府零信任網路廠商說明會

技服中心於 7 月 14 日辦理政府零信任網路廠商說明會，採線上會議方式辦理，會議重點為依據第六期「國家資通安全發展方案(110 年至 113 年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任網路資安防護環境。會中說明政府零信任網路推動政策、期程及需求服務，透過此說明會邀請廠商建立零信任網路之資安供需合作，協同資安公司發展零信任網路資安產業鏈。

政府零信任網路架構主要參考 NIST SP 800-207 零信任架構，結合向上集中防護需求，採取存取門戶部署方式，具備身分鑑別、設備鑑別及信任推斷等 3 大核心機制，身分鑑別包含 FIDO2 身分鑑別與鑑別聲明、設備鑑別則著重於 TPM 設備鑑別與設備健康管理及最後建立基於分數與情境之信任推斷機制。政府零信任網路部署規劃採階段式導入，因此相關組件之部署須具備能與現有系統同時混合運作之能力。依策略階段式導入期程，邀請廠商參與產品驗證，同時技服中心亦於官網建置零信任網路專區，提供相關資訊予機關與廠商參考。

◆ 中央及地方政府資通安全長暨行政院國家資通安全會報委員會議

111 年度中央及地方政府資通安全長暨行政院國家資通安全會報第 39 次委員會議，於 7 月 26 日假台大醫院國際會議中心辦理，會議重點為說明政府機關資安情勢及 111 年資安重點工作，針對政府機關所面臨之多樣態威脅趨勢，相關防護建議包含加強人員資安與機敏資料保護意識、注意重大漏洞訊息並即時進行更新修補及落實委外管理機制。近期資安重點工作為資通系統籌獲各階段資安強化措施，於需求、建置及維運應訂定各項資安

強化措施，以選任適當之受託者，並監督其資通安全維護情形。

會中安排「行動裝置資安風險案例及防護設定」報告，就行動裝置管理框架說明在裝置面、網路面及應用軟體面之資安防護建議，同時因應疫情影響導致居家辦公需求增加，遠距工作者成為駭客主要攻擊對象時，更需強化之行動裝置防護措施，且提醒機關應致力提升使用者資安防護意識。