111年第1季資通安全技術報告

Quarterly Technical Report

目　次

圖 目 次

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 起案例為駭客入侵 Microsoft Teams 會議平台並散布惡意程式；第 2 起案例為駭客利用美國報稅季使用惡意軟體 Emotet，偽冒國稅局名義散布惡意電子郵件。

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 49.62%) 類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 22.56%)」與「網頁攻擊(占 3.01%)」為主要通報類型。

●2.資安專題分享

資安專題分享主題為 OWASP Threat Dragon 威脅模型分析工具簡介，Threat Dragon 為免費開源、跨平台及自動化工具，可運用於資料流程圖(Data Flow Diagram, DFD)繪圖，並根據 DFD 自動產生對應威脅列表，該工具具備 3 種威脅模型類型與改善建議，以視覺化方式呈現系統架構與資安準備狀態。

●3.資安技術研析

資安技術研析主題為 Mozi 殭屍網路攻擊案例分析，分析 Mozi 殭屍網路攻擊手法，包含利用儲存之帳密對物聯網設備進行暴力破解弱密碼攻擊，以擴大感染範圍；另一攻擊手法為利用共通漏洞與暴露(Common Vulnerabilities and Exposures, CVE)漏洞進行攻擊。

●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，了解最新之資安威脅趨勢與因應之資安防護重點。資安專題概述運用 OWASP Threat Dragon 威脅模型分析工具，掌握軟體設計與架構，透過系統化方法識別可能影響資通系統之資安威脅並評估風險，找出系統設計缺陷後，發展對應之資安控制措施。此外，資安技術研析主題為 Mozi 殭屍網路攻擊案例分析，統整分析遭受攻擊裝置類型大多為路由器與網路錄影設備，另有少數網頁應用服務、網路儲存裝置等類型受駭。

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 1 季(以下簡稱本季)透過案例探討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

俄羅斯與烏克蘭戰爭開始之時，數位戰爭亦如火如荼展開，烏克蘭於 1 月 13 日陸續傳出多個政府網站遭大規模駭客入侵，竄改網頁內容且留下恐嚇訊息。由此可見，實體戰爭發生之際，更要特別關注伴隨之數位戰爭，有時甚至數位戰爭所造成之衝擊或影響遠比實體戰爭激烈，如透過網路傳播不實謠言或具體之網路入侵活動。

本季具指標性案例為駭客入侵 Microsoft Teams 會議平台，並散布惡意程式；另一起案例為惡意軟體 Emotet 利用美國報稅季偽冒國稅局名義，散布惡意電子郵件。

首先，探討案例為駭客入侵 Microsoft Teams 會議平台，散布惡意程式並感染協作平台使用者電腦。美國資安業者 Avanan 研究人員警告，駭客利用網路釣魚郵件或藉由入侵組織之合作夥伴等方式，獲取電子郵件帳號或 Microsoft 365 帳號密碼，以成功進入 Microsoft Teams 會議平台，並於使用者間大量散布惡意程式。

據微軟 111 年 1 月統計，每月有超過 2.7 億使用者使用 Microsoft Teams 線上會議平台，惟該平台目前尚未具備針對惡意程式之完整防護措施，且因使用者對 Microsoft Teams 信任度高，導致攻擊案例攀升。研究人員發現，駭客從 111 年 1 月起開始進行攻擊，目前已偵測到數千次攻擊，相關攻擊

案例為駭客將檔名為「User Centric」之惡意程式上傳至聊天室，並誘使其他使用者點選執行。惡意程式一旦執行，將於 Windows 登錄檔寫入資料與安裝 DLL 檔，進而控制受駭電腦。

第 2 起案例為駭客利用美國報稅季使用惡意軟體 Emotet，偽冒國稅局名義散布惡意電子郵件。電子郵件安全業者 Cofense 研究人員發現多個冒充美國國稅局(IRS.gov)之網路釣魚活動，郵件偽裝成國稅局向收件者寄送納稅申請表與其他稅務文件。研究發現這些電子郵件為避免被郵件安全閘道機制偵測發現，會使用有密碼保護之 ZIP 等壓縮檔案或 HTML 檔可連結至 ZIP 壓縮檔，並於內文附上解壓縮密碼。

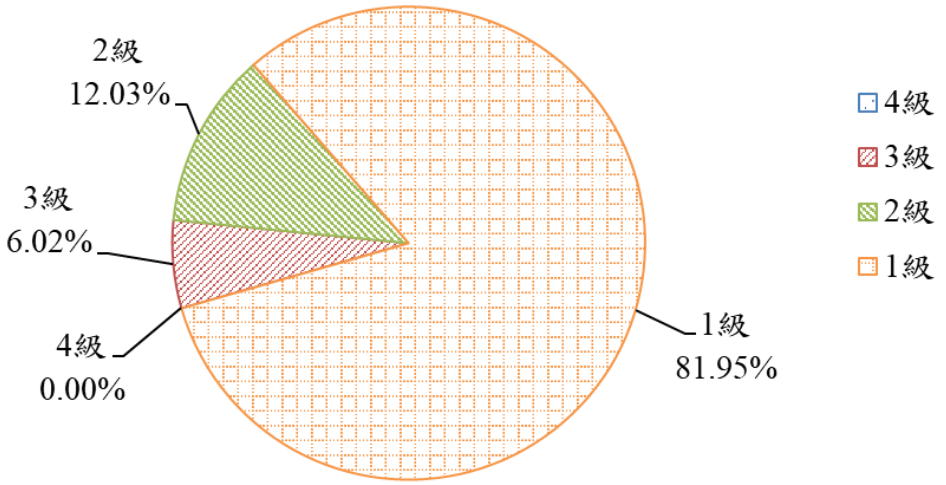
為取得收信者之信任度，這些惡意郵件會在簽名檔加入美國國稅局標識，且部分被鎖定之企業更會在內文提及收信者所屬公司名稱，誘使受駭者開啓郵件所附帶惡意巨集之 Word 或 Excel 檔案。當附件檔案被開啓時，會提示使用者點選「啟用編輯」或「啟用內容」以查看檔案內容，並接續執行惡意巨集，同時從外部遭駭之 WordPress 網站下載並安裝 Emotet 惡意軟體或其他惡意工具，常見有滲透測工具 Cobalt Strike 等，以達成功竊取相關資料或啓動勒索軟體攻擊之目的。.

綜覽本季重大資安事件，疫情方興未艾之際，線上會議需求仍高，因此重要資安課題包含檢視線上會議平台資安防護等級，以及教育使用者辨識與回應惡意行為。借鏡駭客利用美國報稅季利用社交工程郵件入侵使用者電腦，並以勒索軟體攻擊或竊取資料事件，國內亦應利用多方管道加強資安意識宣導，降低駭客入侵之機率。

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 81.95%為大宗，2 級事件占 12.03%次之，3 級事件僅占 6.02%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。



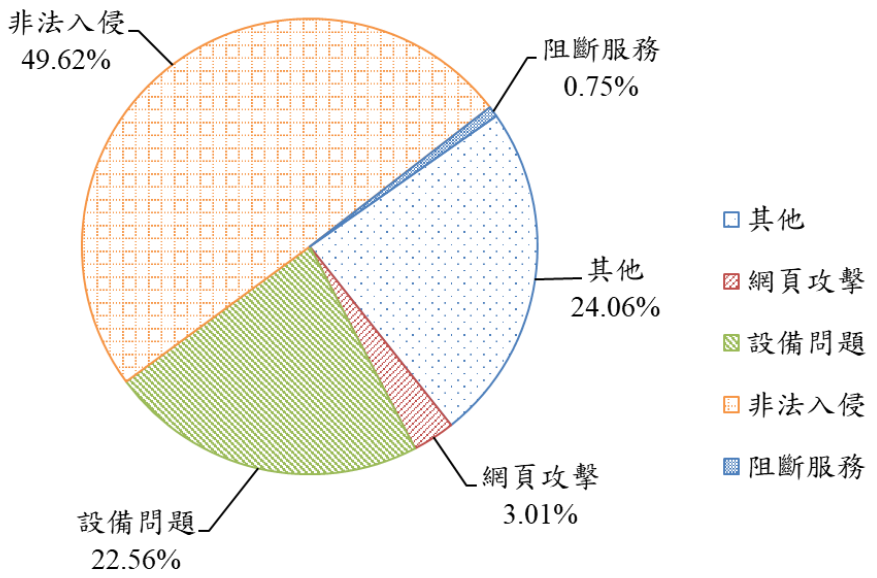
資料來源：本報告整理

圖1　111 年第 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，主要為個人資料外洩與涉及核心資通系統服務中斷等事件。個人資料外洩事件係因機關管理社群媒體之管理者帳號密碼外洩，而該粉絲專頁私人對話訊息存在抽獎活動之中獎者個人資料。另外，政府計畫之個人資料檔案遭竄改，經調查後發現不僅個人資料檔案遭竄改刪除，公告訊息亦遭異動。核心資通系統服務中斷事件原因為電力中斷，或因資料庫毀損無法正常運作等因素，造成核心資通系統無法可容許回復時間內恢復運作。

除上述資安事件外，技服中心亦偵測多個機關疑似遭社交工程郵件攻擊成功，植入殭屍網路惡意程式。雖政府機關已普遍進行社交工程演練，惟現今社群媒體發達，再加上駭客善於利用時事議題變換攻擊手法，使用者更應步步為營加強防範相關社交工程攻擊。整體事件比率，以「非法入侵」

(占 49.62%)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。



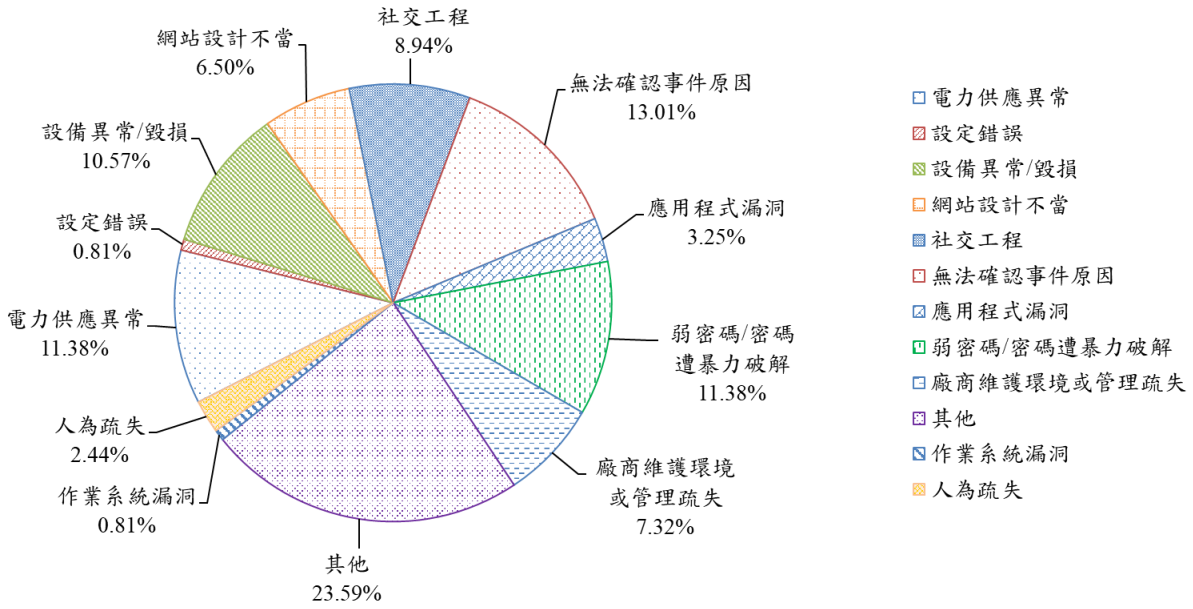
資料來源：本報告整理

圖2　111 年第 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電力供應異常(11.38%)、弱密碼/密碼遭暴力破解(11.38%)、設備異常/毀損(10.57%)、社交工程(8.94%)、廠商維護環境或管理疏失(7.32%)、網站設計不當(6.50%)、應用程式漏洞(3.25%)、人為疏失(2.44%)、設定錯誤(0.81%)及作業系統漏洞(0.81%)。分析本季事件，「電力供應異常」主因為電廠電力中斷，造成資通系統可用性無法滿足。電廠人員進行設備測試時，因人為操作疏失造成電力系統設備毀損，部分機關因停電影響，造成資通系統可用性遭受衝擊而進行事件通報。

事件發生原因若無法符合現行特定類別將歸屬至「其他」類，機關人員自行下載非公務使用之軟體，因該程式夾帶有惡意檔案，故通報資安事件。另一案例為發現攻擊來源為開放給民眾使用之無線網路(WIFI)網段，惟因無法釐

清連線設備，判斷可能來自於民眾自攜設備，故無法進一步追查。



資料來源：本計畫整理

圖3　111 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，駭客利用因疫情而興起之遠端連線平台，趁使用者信賴品牌公司所提供之平台，且尚未完全熟悉軟體操作狀況下展開攻擊，同時運用時事議題發展之社交工程攻擊，更讓人防不勝防。因此，在使用任何資訊設備或平台前皆應先評估其資安防護措施與等級，同時應加強教育使用者風險意識。

政府案例中有一個資外洩事件為使用者個人電腦遭植入惡意程式後，所儲存之雲端服務帳號密碼被竊取進而遭入侵，且其儲存於雲端之公務個人資料與內部系統之帳號密碼亦被上傳至暗網。此類案件除應請當事人立即變更雲端服務之密碼外，亦應阻擋可疑連線，進行端點鑑識並持續觀察。

綜整以上資安威脅現況，提供資安防護建議如下：

●雲端服務之資安管理

– 定義使用雲端服務之資安管理責任，設定安全組態基準值。

– 機敏性資訊應避免存放於雲端，必須儲存於雲端時應進行資料加密。

– 發生資安事件時，應教育使用者即時啓動通報與應變程序。

●線上會議平台之資安管理

– 針對所有商業通訊軟體皆須部署資安防護與偵測機制，包含 Microsoft Teams 等。

– 建置沙盒安全機制檢視線上會議平台所下載之檔案，並確認其內容是否有惡意程式。

– 建立弱點通報機制，平台協作之使用者一旦發現可疑之與會者或檔案時，應立即通報。

●社交工程郵件之資安管理

– 教育使用者不開啓來源不明之信件或附件，並關注官方宣導之資安訊息。

– 關閉 Office 系列之自動啟用巨集功能，避免惡意程式透過巨集感染收件人電腦。

– 若收到疑似夾帶 Emotet 惡意附檔之電子郵件時，可利用 Emotet Malspam 資料庫(https://www.haveibeenemotet.com/)，查詢寄件人電子郵件地址是否涉及發送 Emotet 垃圾郵件。

2. 資安專題分享_OWASP Threat Dragon 威脅模型分析工具簡介

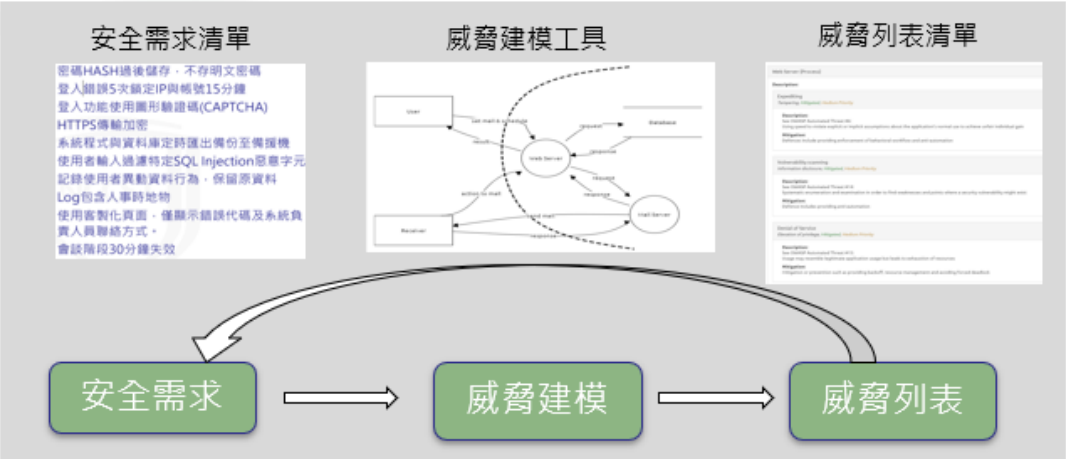
資安事件中不乏出現系統漏洞，致被入侵、營運中斷及資料外洩等，歸究其可能因素包含程式需求分析錯誤、設計疏失、上線前未經安全測試、變更管理程序疏漏及未及時偵測系統弱點等。相關風險辨識，不僅需於專案初始時期即了解威脅全景，更需要反覆測試與熟悉於每一系統開發階段可能面臨之資安議題。

傳統系統發展流程偏重功能需求，普遍缺乏資安設計考量，為有效提升資通系統安全發展流程與技術，需依賴自動且便捷之建構知識庫、模型及工具。安全系統發展生命週期(Secure System Development Lifecycle, SSDLC)方法論強調從專案開始各階段及早加入資安思維，打造具備資安體質之資通系統。設計階段依據系統功能與需求進行威脅建模(Threat Modeling)，以識別可能影響系統之資安威脅。系統開發亦需遵循法規之要求，資通安全管理法之「資通系統防護基準」規定，中風險等級以上之資通系統應於系統發展生命週期設計階段，根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。

以下將針對威脅建模(Threat Modeling)與 OWASP Threat Dragon 威脅建模工具進行簡介，並進行應用案例實測。

2.1 威脅建模與 OWASP Threat Dragon 專案概述

威脅建模主要用於對軟體設計與架構掌握，透過系統化方法識別可能影響資通系統之資安威脅並評估風險，找出系統設計缺陷後，對應發展資安控制措施，詳見圖 4。



資料來源：本報告整理

圖4　威脅建模流程

系統開發者可經由威脅建模工具，產生潛在威脅列表，透過檢視各項威脅是否有對應之安全性需求，或新增安全性需求，以確認所有威脅皆已減緩。系統開發期間，持續進行相關流程，以提供其安全程度。商用威脅模型分析方式以微軟提出以攻擊者導向為主之 STRIDE，分別從帳密破解等身分偽冒攻擊(Spoofing)、資料庫內容竄改等攻擊(Tampering)、日誌紀錄不足等否認性(Repudiation)、機敏資訊外洩等攻擊(Information Disclosure)、阻斷服務攻擊(DoS)及提權行為(Elevation of Privilege)。

Threat Dragon 為免費開源、跨平台及自動化工具，提供平台之桌面版與網頁版使用。自 103 年開始發展後，現已成為 OWASP 實驗室專案(Lab Project)，該專案之發展主要目的為威脅模型應用。此工具可運用於資料流程圖(Data Flow Diagram, DFD)繪圖，並根據 DFD 自動產生對應威脅列表，包含 3 種威脅模型類型與改善建議，且其報表功能以視覺化方式呈現系統架構與資安準備狀態。

2.2 OWASP Threat Dragon 應用案例實測

應用案例實測目的為用 Threat Dragon 進行威脅建模分析，確認其可行性。以常見之「Web Mail 系統」為例，主要步驟分別為預先規劃系統資安需求、根據系統架構畫出威脅模型圖、透過 Threat Dragon 產生威脅列表，之後針對威脅列表進行風險分析與威脅緩解，並調整或新增相關資安需求，以持續強化資通系統防護韌性。

實測時先選定數項系統發展生命週期需求階段規劃之資安需求，包含密碼 HASH 過後儲存，不存明文密碼、登入錯誤 5 次鎖定 IP 與帳號 15 分鐘、密碼變更時，至少不可以與前 3 次使用過之密碼相同、登入功能使用圖形驗證碼(CAPTCHA)及 HTTPS 1.2 傳輸加密等。

從分析步驟 1 開始進行威脅模型圖元素拆解，分析系統架構，拆解系統組成元素，再搭配系統使用情境，分析資料流與信任邊界，詳見圖 5。

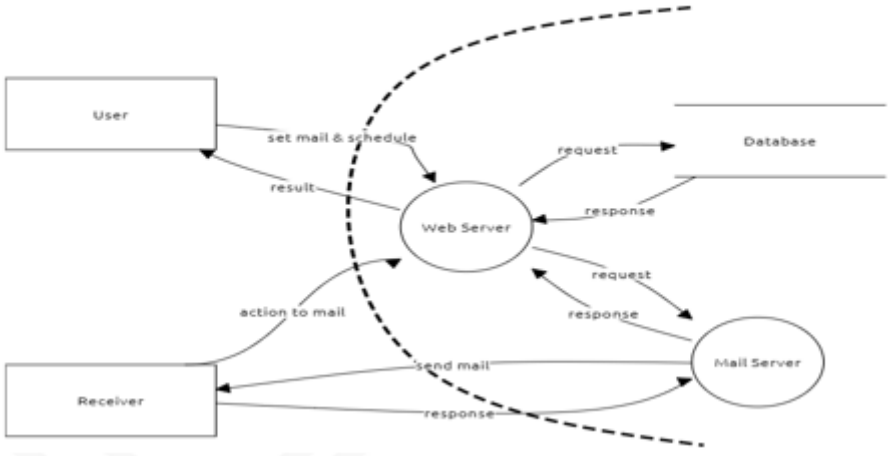
Process	Store	Actor
• Web Server • Mail Server	• Database	• User • Receiver

Data Flow			
User	Receiver	Web Server	Mail Server
→Web Server (應用程式設定信件內容、寄發人員、寄發時間)	→Web Server (操作信件功能、發送訊息)	→Database (設定資訊內容) →Mail Server (寄發時間寄送信件資訊)	→Receiver (寄信)

資料來源：本報告整理

圖5　威脅模型圖元素拆解

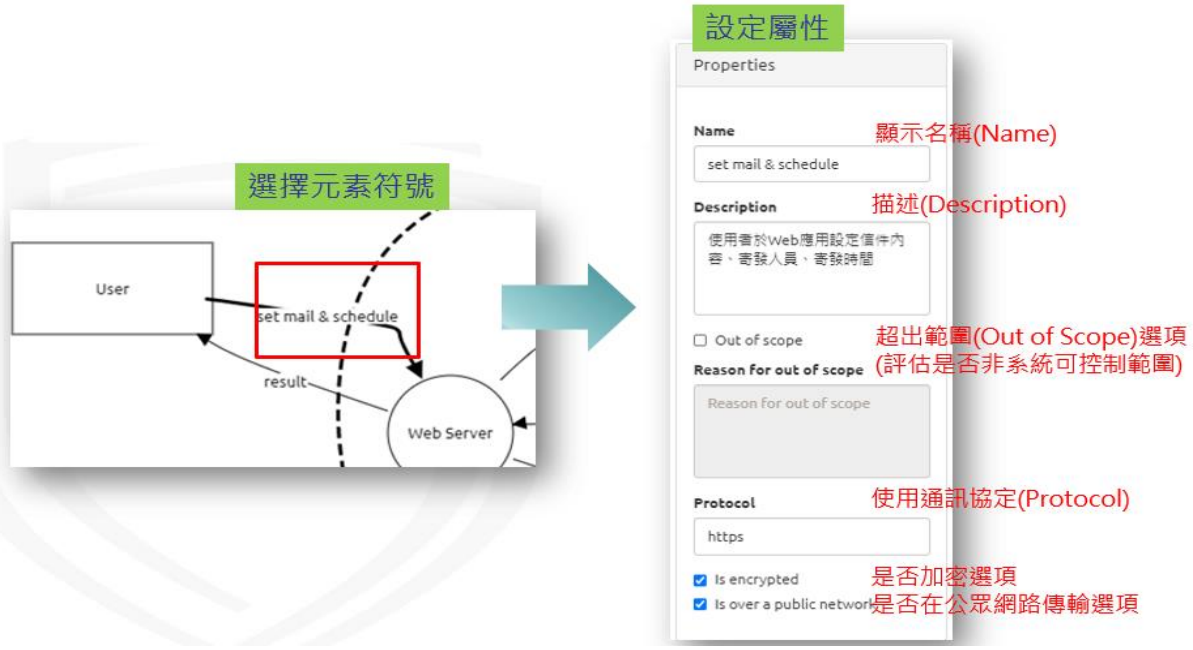
分析步驟 2 則繪製威脅模型圖，依據步驟 1 拆解元素，組合繪製威脅模型圖，詳見圖 6。



資料來源：本報告整理

圖6　繪製威脅模型圖構

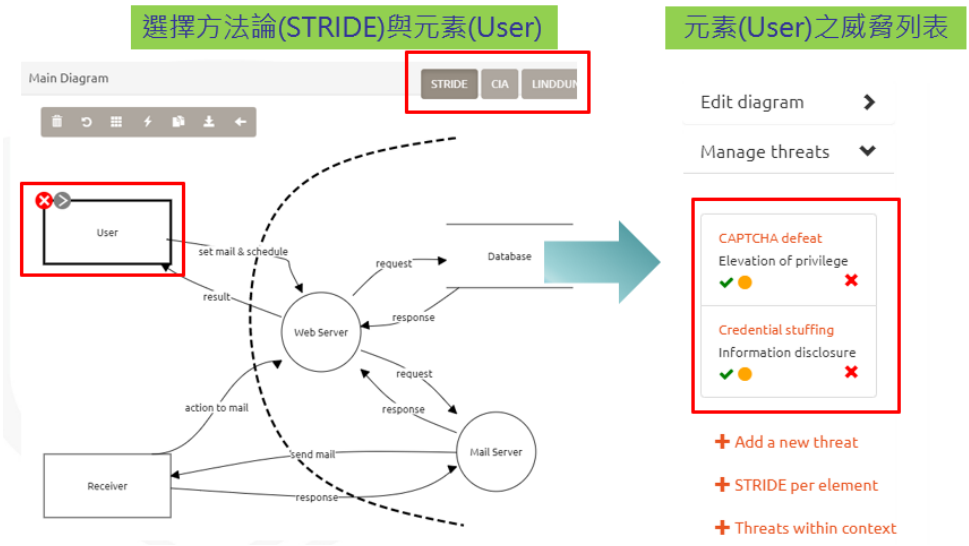
分析步驟 3 為設定威脅元素屬性，針對威脅模型圖，個別設定元件屬性。以 User 至 Web Server 傳輸資料流設定為例，設置控制範圍、使用協定、加密等屬性選項，詳見圖 7。



資料來源：本報告整理

圖7　威脅元素屬性設定

分析步驟 4 產製威脅列表，主要工作項目為選擇分析方法論與元素，依個別產製元素威脅列表，詳見圖 8。



資料來源：本報告整理

圖8　產製威脅列表

分析步驟 5 為檢視威脅與緩解，逐一檢視威脅列表內容，可設置威脅處理狀況，並查閱威脅細節與緩解措施。此工作項目可利用產出之報告與清單，協助開發者進行程式設計缺陷之修復與驗證，詳見圖 9。

資料來源：本報告整理

圖9　威脅與緩解措施對應

步驟 6 為調整或新增相關資安需求，以「Web Mail 系統」案例實測結果，在逐一檢視所有威脅，並確認是否建置相關資安需求控制措施後，發現需增加「登入帳號使用多因子驗證」。

依此實測，最後步驟將資安需求或控制措施文件化，並追蹤實作及測試成果以驗證其有效性。OWASP Threat Dragon 為免費開源之威脅建模工具，支援之資安威脅分析方法類型多，且為跨平台並支援網頁版可集中控管，機關可評估使用此工具納入威脅建模，以強化於安全系統發展生命週期(Secure System Development Lifecycle, SSDLC)設計階段之安全性。

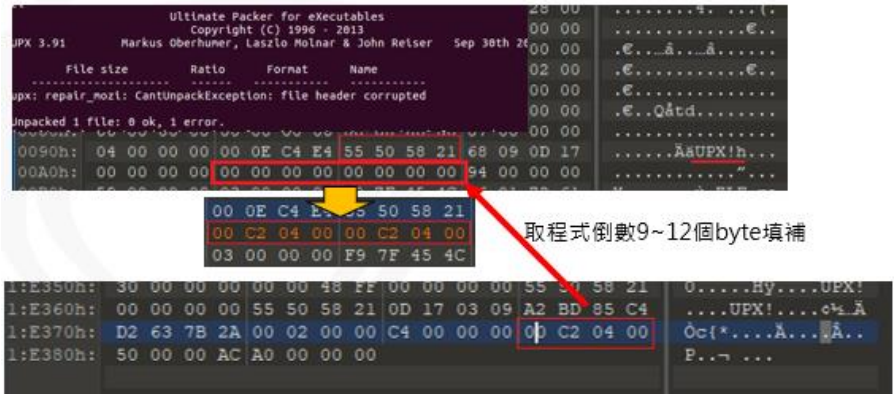
3. 資安技術研析_Mozi 殭屍網路攻擊案例分析

本季探討之資安技術研析為 Mozi 殭屍網路攻擊案例分析，Mozi 殭屍網路最早於 108 年被發現進行攻擊活動，特點為使用分散式雜湊表(Distributed Hash Table, DHT)協定之點對點(Peer to Peer, P2P)殭屍網路，以廣泛運用分散在網際網路上之各項資源。韓國國家情報院(National Intelligence Service, NIS)於 110 年 12 月檢測發現，迄今全球仍有約 12,000 台設備遭 Mozi 殭屍網路感染，其主要攻擊目標類型為路由器、網通設備及數位視訊錄影機(Digital Video Recorder, DVR)等物聯網裝置。

技服中心於 111 年 1 月接獲情資平台 Malware URL Exchange 通報，發現台灣境內之 Mozi 殭屍網路惡意下載站。因此，依情資提供之活動紀錄時間，以最新活動下載站之惡意樣本進行分析，以下將針對 Mozi 殭屍網路攻擊概覽與惡意程式進行分析說明。

3.1 Mozi 殭屍網路樣態分析

進行惡意程式分析前，發現該程式已使用免費之壓縮加殼工具 UPX 進行加殼，並利用空值覆蓋 UPX 之 p_filesize、p_blocksize 內容以防止其他人分析，因此需透過手動填補方能順利脫殼分析，詳見圖 10。



資料來源：本報告整理

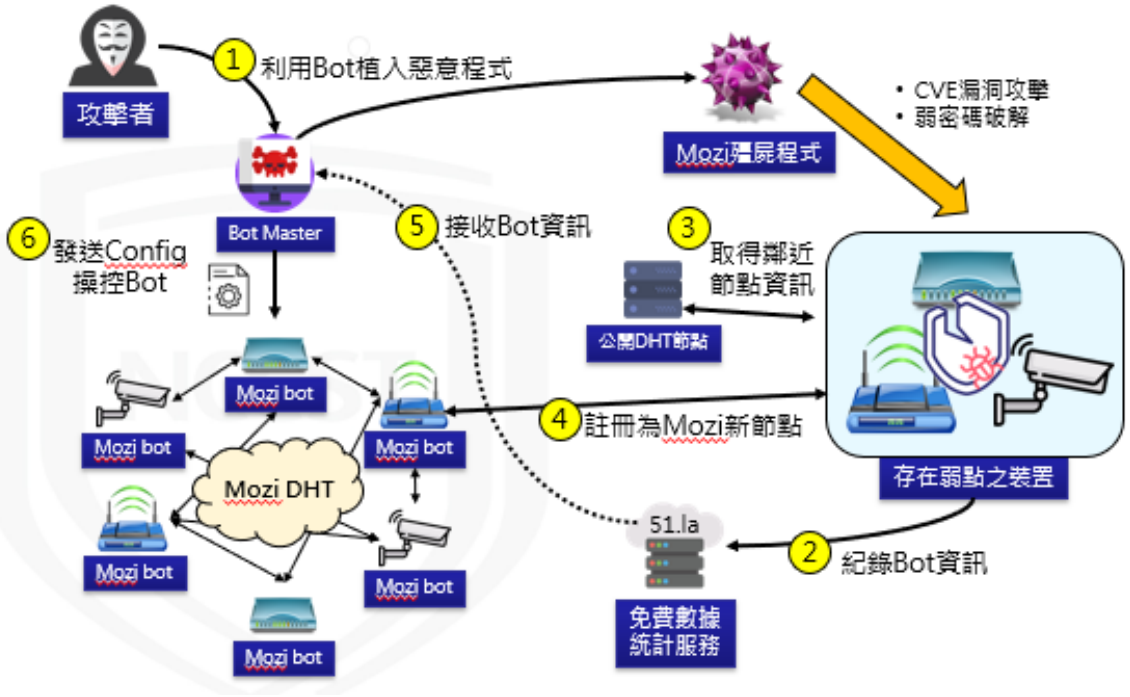
圖10 反逆向分析之加殼處理

Mozi 殭屍網路偏好鎖定安全性較低之設備，針對使用弱密碼或已知漏洞之資通系統展開攻擊，目的為擴大感染殭屍網路範圍。後續憑藉已遭受感染之設備做為跳板，以發動分散式阻斷服務(Distributed Denial of Service, DdoS)攻擊。常見案例之一為感染物聯網設備，如路由器等，攻擊方式為劫持進行中間人攻擊(Man In The Middle, MITM)或網域名稱伺器欺騙(Domain Name System Spoofing, DNS Spoofing)。

對 Mozi 殭屍網路惡意程式樣本進行分析，發現存有特定廠牌設備之登入帳號與密碼字串，其中包含華為、居易科技、銳捷科技等廠牌之設備帳密，推測 Mozi 殭屍網路利用儲存之帳密對相關設備進行暴力破解弱密碼攻擊，以擴大感染範圍。另一攻擊手法為利用共通漏洞與暴露(CVE)漏洞攻擊，逆向分析樣本後，發現帶有多個 HTTP 漏洞攻擊 Payload，目標鎖定多款物聯網設備成為主要擴散感染途徑，經整理 Mozi 殭屍網路，共發現約 10 種漏洞攻擊工具，漏洞攻擊之目標類型包含 Dasan GPON、華為、Eir 及 Netgear 等網通設備，以及 MVPower、Vacron 等視訊設備。

3.2 Mozi 殭屍網路攻擊手法與過程分析

分析 Mozi 殭屍網路樣本時，發現程式 Mozi 殭屍網路樣本中包含之字串與 Mirai 殭屍網路公開程式碼有相同特徵，由此推斷 Mozi 殭屍網路應使用 Mirai 殭屍網路部分程式修改而來，綜整其攻擊方式與流程概覽，詳見圖 11。



資料來源：本報告整理

圖11 Mozi 殭屍網路攻擊方式與流程概覽

成功感染目標設備後，Mozi 殭屍網路會建立防火牆阻擋 SSH 與 Telnet 服務之連線埠，以防止競爭之殭屍網路入侵設備，詳見圖 12。

以iptables指令建立防火牆規則

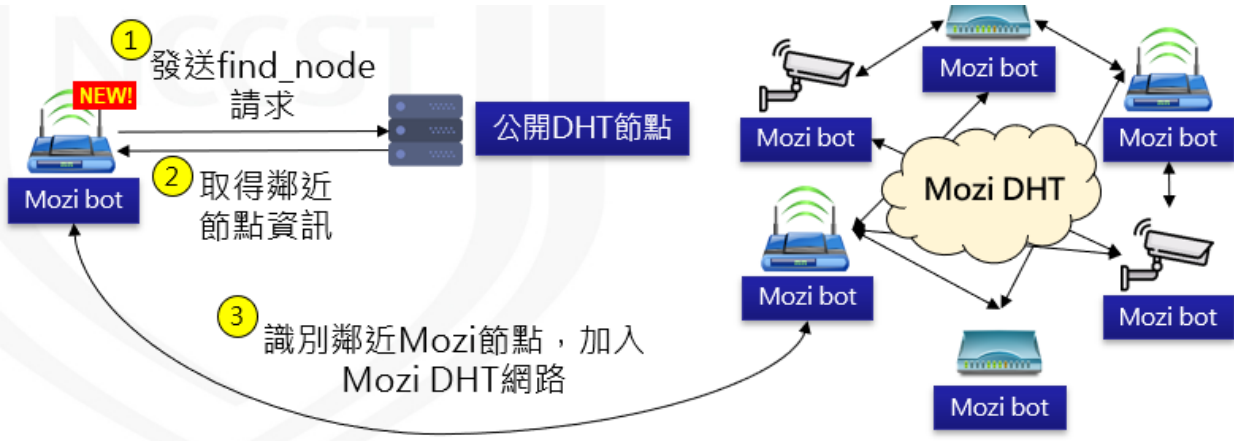
```
exec_bash((int)"iptables -I INPUT  -p tcp --destination-port 22 -j DROP");
exec_bash((int)"iptables -I INPUT  -p tcp --destination-port 23 -j DROP");
exec_bash((int)"iptables -I INPUT  -p tcp --destination-port 2323 -j DROP");
exec_bash((int)"iptables -I OUTPUT -p tcp --source-port 22 -j DROP");
exec_bash((int)"iptables -I OUTPUT -p tcp --source-port 23 -j DROP");
exec_bash((int)"iptables -I OUTPUT -p tcp --source-port 2323 -j DROP");
exec_bash((int)"iptables -I INPUT  -p tcp --dport 22 -j DROP");
exec_bash((int)"iptables -I INPUT  -p tcp --dport 23 -j DROP");
exec_bash((int)"iptables -I INPUT  -p tcp --dport 2323 -j DROP");
exec_bash((int)"iptables -I OUTPUT -p tcp --sport 22 -j DROP");
exec_bash((int)"iptables -I OUTPUT -p tcp --sport 23 -j DROP");
exec_bash((int)"iptables -I OUTPUT -p tcp --sport 2323 -j DROP");
```

資料來源：本報告整理

圖12 建立防火牆規則防止競爭之殭屍網路

除此之外，Mozi 殭屍網路亦會關閉 Telnet 與遠端管理之系統程式等相關服務，以防止競爭者干擾。

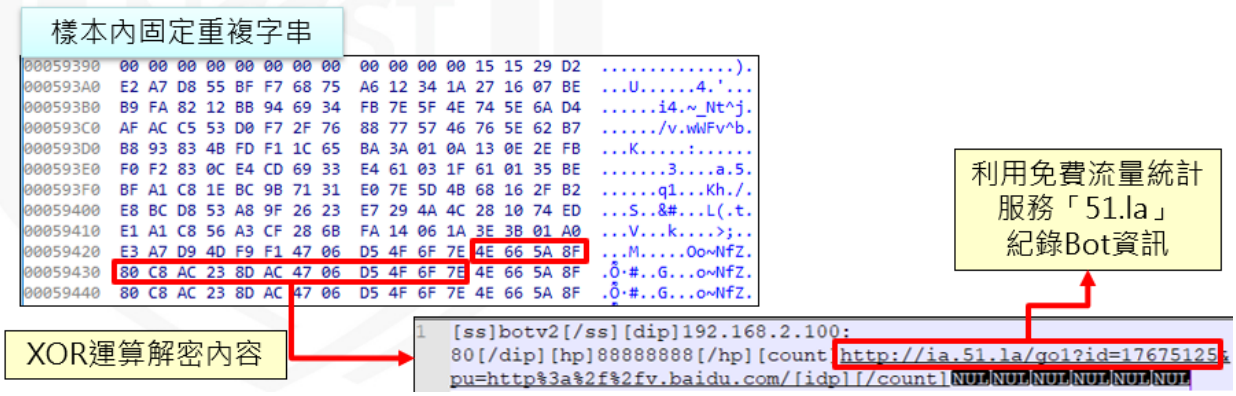
進一步分析 Mozi 殭屍網路 DHT 網路運作流程，因 Mozi 殭屍網路是屬於 P2P 類型之殭屍網路，連線活動以 DHT 協議進行通訊，一個節點加入 DHT 網路時，需先取得網路中之任意節點，新成立之 Mozi 殭屍網路節點，會向樣本內儲存之 DHT 公開節點發送「find_node」請求，以查詢鄰近之節點資訊，進而加入 DHT 網路，詳見圖 13。



資料來源：本報告整理

圖13 DHT 網路運作流程

樣本內共儲存 7 個 DHT 公開節點位置，樣本以固定字串「888888」加上隨機字串，產生自身節點之識別 ID。從流量觀察發現，樣本將節點 ID 發送至 DHT 公開節點，並取得鄰近節點之 ID 資訊。樣本會產生「.config」檔案，用於註冊 Mozi 殭屍網路新節點。「.config」內容已加密，利用樣本發現之固定重複字串做為金鑰，以 XOR 運算可解密內容，詳見圖 14。

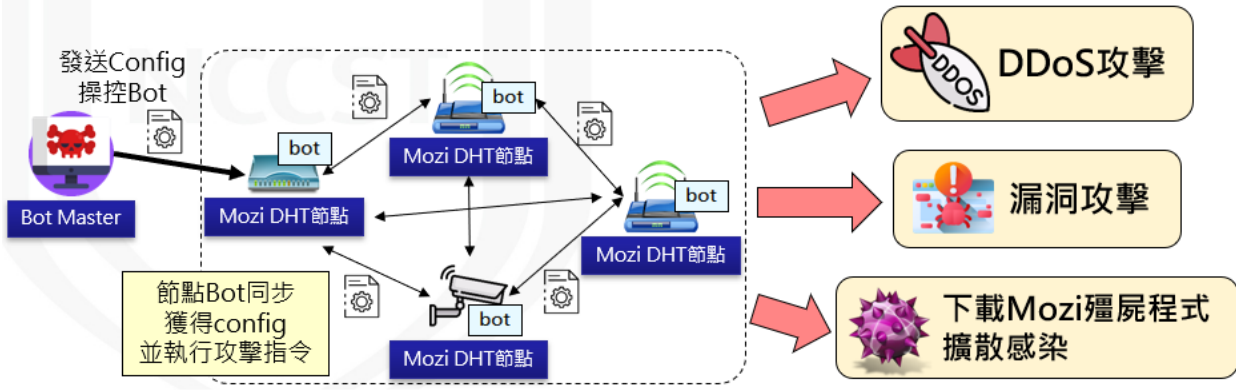


資料來源：本報告整理

圖14 利用 XOR 解密內容

基於 Mozi 殭屍網路採用 P2P 網路架構之特性，駭客為進一步掌控感染數量，利用免費流量統計服務「51.la」，做為上傳 Bot 資訊之中繼伺服器，由其後臺分析 IP 來源與設備系統資訊等數據。

進階分析 Mozi 殭屍網路控制 P2P 殭屍網路之手法，Mozi 殭屍網路以 DHT 建立之 P2P 殭屍網路，是利用 Bot Master 發送 config 檔案，控制 Mozi 殭屍網路節點之殭屍設備執行攻擊任務。由 Bot Master 發送 config 檔案至鄰近節點，且 Mozi 殭屍網路 DHT 網路內所有節點會同步獲得 config，詳見圖 15。



資料來源：本報告整理

圖15 利用 Mozi 殭屍網路控制 P2P 殭屍網路之手法

Mozi 殭屍網路發送之 config 內容，包含多個指令用於設定 Bot、控制 Bot 設備及派送執行之任務。

分析攻擊跳板發現大多為 Mozi 殭屍網路感染之受駭裝置，來源主要以中國、印度及俄羅斯為主，受駭裝置之 ISP 主要為一般電信業者，來源國家以中國居多。統整分析遭受攻擊裝置類型大多為路由器與網路錄影設備，另有少數網頁應用服務、網路儲存裝置等類型受駭。

管理者除持續觀察 Mozi 殭屍網路活動情況，應及時檢視所使用設備之資通系統防護基準、組態設定及更新狀態，以防範 Mozi 殭屍網路攻擊。

4. 結論

本季具指標性案例為駭客入侵 Microsoft Teams 會議平台，散布惡意程式並感染會議平台之使用者電腦。因使用者普遍對 Microsoft Teams 信任度高，導致攻擊案例攀升，駭客入侵手法包含利用網路釣魚或藉由入侵組織之合作夥伴等方式，獲取電子郵件帳號或 Microsoft 365 憑證，以成功進入 Microsoft Teams 會議平台散布惡意程式。第 2 起案例為為駭客利用美國報稅季使用惡意軟體 Emotet，偽冒國稅局名義散布惡意電子郵件，並在簽名檔加入美國國稅局標識以取信收信者，一旦受駭者開啓郵件所附帶惡意巨集之 Word 或 Excel 檔案後，將自動執行惡意程式。

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「雲端服務之資安管理」與「線上會議平台之資安管理」及「社交工程郵件之資安管理」，提出資安防護建議。

資安專題分享主題為 OWASP Threat Dragon 威脅模型分析工具簡介，概述 Threat Dragon 工具之特色與功能性，並運用此工具進行威脅建模分析之應用案例實測，以確認其可行性。主要步驟分別為預先規劃系統資安需求、根據系統架構畫出威脅模型圖、透過 Threat Dragon 產生威脅列表，之後針對威脅列表進行風險分析與威脅緩解，並調整或新增相關資安需求，以持續強化資通系統防護韌性。

另外，資安技術研析主題為 Mozi 殭屍網路攻擊案例分析，以情資提供之活動紀錄時間，針對最新活動下載站之惡意樣本進行分析。逆向分析樣本後，發現帶有多個 HTTP 漏洞攻擊 Payload，目標鎖定多款物聯網設備成為主要擴散感染途徑，共發現約 10 種漏洞攻擊工具，漏洞攻擊之目標類型包含網通設備與視訊設備等。