110年第4季資通安全技術報告

Quarterly Technical Report

目　次

圖 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，提供政府機關最新資安風險之關注重點。

「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 起案例為利用重大漏洞 Log4Shell 攻擊態勢加劇；另一起案例為殭屍網路惡意程式利用老舊漏洞，攻擊物聯網裝置。

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 61.02%)」類型為主，排除綜合類型「其他」外，其次分別為「設備問題(占 11.3%)」與「網頁攻擊(占 6.78%)」為主要通報類型。

●2.資安專題分享

資安專題分享主題為網路儲存裝置之資安攻擊與防護，說明駭客如何利用漏洞進行攻擊與入侵，影響後果包含設備資料遭勒索加密、使用系統資源進行挖礦及造成資料毀損等。

●3.資安技術研析

資安技術研析主題為 Mozz 殭屍網路攻擊案例分析，Mozz 殭屍網路使用企業應用軟體與視訊設備之漏洞進行攻擊與擴散感染，針對開源內容管理系統 Drupal 之漏洞進行攻擊，注入微型惡意腳本。

●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。資安專題分享網路儲存裝置之資安攻擊與防護，了解駭客如何利用漏洞進行攻擊與入侵，進而展開勒索加密、使用系統資源進行挖礦及造成資料毀損等行為。此外，Mozz 殭屍網路攻擊案例分析，利用應用軟體與視訊設備之漏洞進行攻擊、擴散感染及挖礦行為。

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 4 季(以下簡稱本季)探討系統未更新風險、如何加強資通系統組態設定與維護及個資欄位遮蔽保護，以降低資安事件發生。

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

現實生活中，新冠病毒不斷變種，嚴重影響所有經濟與民生活動。同樣地，在虛擬環境中，駭客利用各種不同途徑與弱點步步逼近，亦讓管理者疲於奔命。當防疫成為日常，期待防駭亦能成為生活顯學。

本季具指標性案例為重大漏洞 Log4Shell 攻擊態勢加劇；另一起案例為殭屍網路惡意程式利用老舊漏洞，攻擊物聯網(Internet of Thing, IoT)裝置。

首先，探討案例為利用重大漏洞 Log4Shell 攻擊態勢加劇。廣泛使用於各種產品與服務之日誌程式庫 Log4j 被發現 Log4Shell 之重大漏洞，漏洞被揭露後，攻擊者已開始利用該漏洞展開各種攻擊，如安裝加密挖礦程式、竊取系統憑證及竊取資料等。受駭者包含亞馬遜雲端服務、谷歌雲端服務、微軟、思科及 IBM 等主要科技公司，均發現其部分產品與服務因受 Log4Shell 漏洞影響而遭到攻擊。相關攻擊擴展至國防單位，據比利時當地媒體報導，比利時國防部證實因 Apache Log4j 軟體安全漏洞遭到攻擊，致網路服務中斷。

Log4Shell 漏洞亦可能對工業控制系統之營運科技(Operational Technology, OT)產生重大影響，據分析駭客可能利用 Log4Shell 漏洞，攻擊使用 Java 開發之廠商專有監控、資料擷取系統與能源管理系統，若成功入侵影響甚鉅。

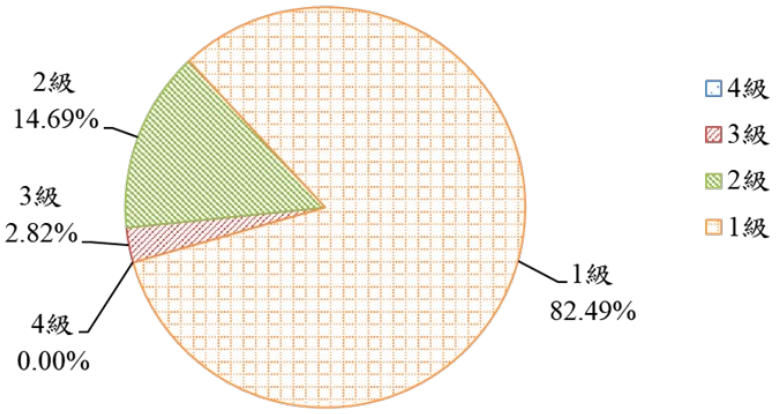
第 2 起案例為殭屍網路惡意程式利用老舊漏洞，攻擊 IoT 裝置。大型電信

業者 AT&T 之資安實驗室 Alien Labs 揭露新殭屍網路惡意程式 BotenaGo，利用 33 個已知之老舊資安漏洞，鎖定數百萬台 IoT 設備發起攻擊行動，相關設備包含網路路由器、數據機、網路儲存裝置等，其中有部分受駭裝置是由台灣廠商生產製造。BotenaGo 使用程式語言 Go 撰寫，成功入侵設備後會執行遠端 Shell 指令，並依受感染設備類型，下載不同惡意封包資料(Payload)，駭客現已刪除伺服器上所有惡意封包資料，使資安研究人員無法得知駭客最終企圖。

綜覽本季重大資安事件，Log4Shell 重大漏洞被揭露後，因日誌程式庫 Log4j 被廣泛使用於各種產品與服務，使用人數眾多且極易被觸發，攻擊對象涵蓋知名企業，如 Google、Apple、Amazon 及 Tesla 等，造成影響廣泛，也被預測恐將影響數年之久。另外，惡意程式利用系統漏洞之事件屢見不鮮，再再顯示系統即時更新之重要性。

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」等 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 82.49%為大宗，2 級事件占 14.69%次之，3 級事件僅占 2.82%，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 4 季通報事件影響等級比率圖

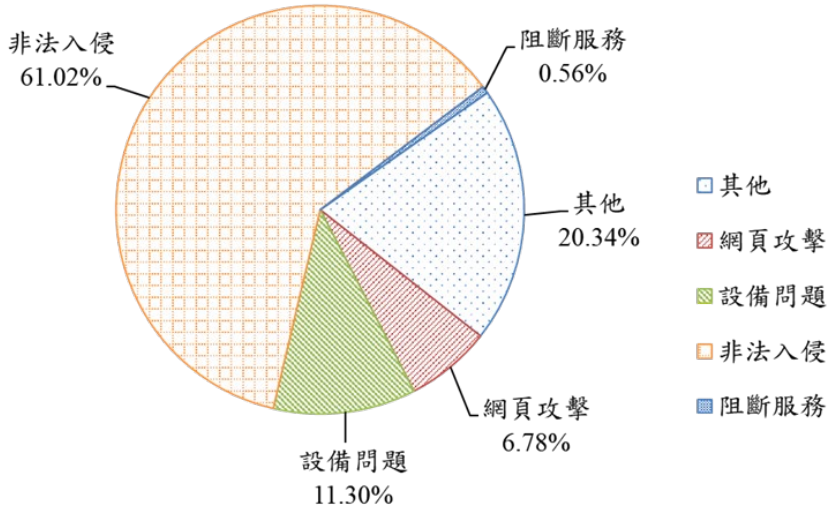
本季接獲之 3 級重要通報事件，以個人資料外洩事件居多，發生肇因概分為 2 種，包含承辦人員不慎誤將未遮蔽之個人資料上傳至公開網站，以及網站活動報名資料外洩等狀況。因個資外洩事件，除有當事人反映該個資被公開至海外伺服器外，亦陸續傳出接獲詐騙電話等。

另一需要探討之 3 級事件為發生在關鍵基礎設施提供者之系統維護事件，辦理主機版本提升維護作業時，因系統衝突影響，致服務中斷。另一起類似事件為廠商進行測試資料回傳時，誤傳至正式主機，致資料錯誤，經調整網路設備設定後，已完成相關測試作業。相關事件因影響核心業務或核心資通系統中斷，歸類為 3 級事件。

除上述資安事件外，本季持續有機關因在安裝 oCam 免費螢幕錄影軟體時，亦一併安裝該軟體之贊助挖礦程式 BRTSvc，導致機關對外連線礦池。雖然最新 oCam 版本 v.520 已不再預設勾選安裝挖礦程式，惟若先前已下載 oCam，則須手動移除該挖礦程式。其他類似挖礦事件則因機關未更新 QNAP 網路儲存系統版本，導致駭客利 Helpdesk 軟體漏洞而植入挖礦程式。

統計本季通報事件類型，以「非法入侵(占 61.02%)」類型為主，排除綜合類

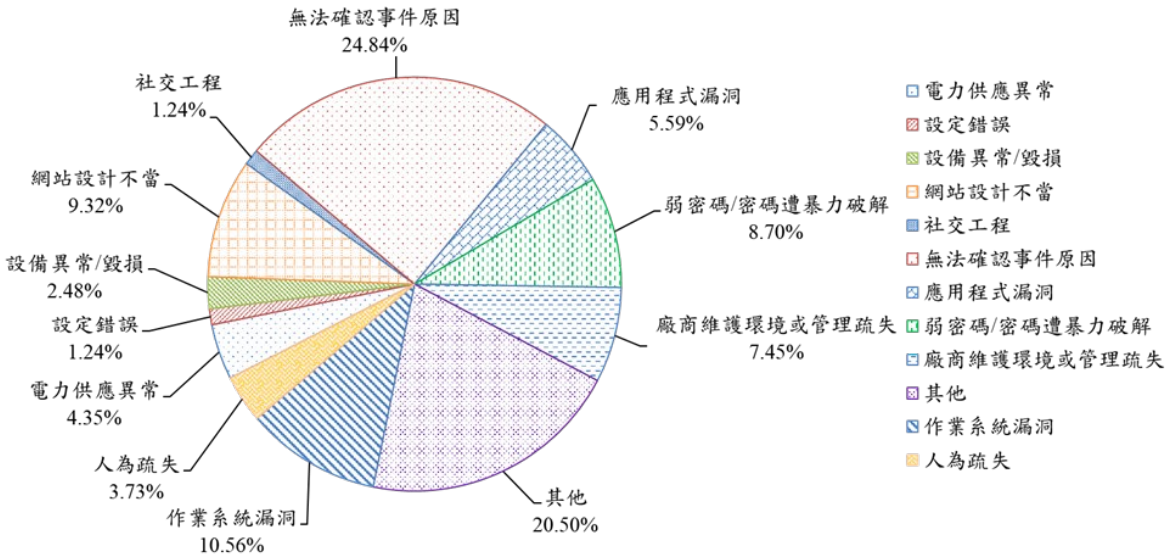
型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　110 年第 4 季通報類型比率圖

進一步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作業系統漏洞(10.56%)、網站設計不當(9.32%)、弱密碼/密碼遭暴力破解(8.70%)、廠商維護環境或管理疏失(7.45%)、應用程式漏洞(5.59%)、電力供應異常(4.35%)、人為疏失(3.73%)、設備異常/毀損(2.48%)、設定錯誤(1.24%)及社交工程(1.24%)。觀察本季事件發生原因，作業系統漏洞為駭客族群鑽研漏洞存在與否之首要目標，故為常見之駭客入侵途徑，從事件中可見作業系統漏洞造成事件發生原因占居首位。雖然要求作業系統更新早已成為資安防護之重點項目，惟如何落實更新與檢核機制仍有進步空間。



資料來源：本計畫整理

圖3　110 年第 4 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，Log4Shell 於漏洞評分系統之危險等級相當高，又因其使用者眾多及易被觸發之特性，不論是政府機關或企業皆高度重視。面對層出不窮之系統漏洞，更應全面並定期檢視所使用之系統是否存在漏洞與缺失，積極更新。

國內因作業系統漏洞而發生之資安事件亦占居首位，顯見系統漏洞問題亦應由管理者思考與規劃有效措施，以降低資安事件之發生。另外，國內常見之個資外洩事件，不論是機關本身或委外廠商都屢見因個資未妥善處理導致外洩之事件。負責個資處理之人員應具備個資管理相關觀念，如個人資料應視為敏感資訊，同時由機關提供個資管理規範供參考，方可逐漸減少相關事件之發生。另外，核心資通系統因設定錯誤或人為疏失造成之服務中斷，足見維運或測試作業流程尚有改善空間。

綜整以上資安威脅現況，提供資安防護建議如下：

●IoT 裝置之資安管理

– 盤點內部 IoT 裝置，確認使用目的、連線範圍及管理人員後列冊管理。

– 依風險評鑑結果訂定資安使用原則，並定期檢視系統弱點與更新週期。

●個資遮蔽與保護之資安管理

– 依個資不同欄位討論遮蔽原則，並確認其於資料生命週期之管理一致性。

– 訂定稽核驗證原則，定期檢視個資遮蔽之有效性。

●組態設定與系統變更之資安管理

– 訂定組態設定之資安管理規範，依序檢視可能影響事項或衝擊後再執行變更處理，並規劃系統變更失敗時之復原點。

– 定期檢視組態設定之原則與例外處理事項，以確認符合資通系統資安要求。

2. 資安專題分享_網路儲存裝置資安攻擊與防護

近期網路儲存裝置(Network Attached Storage, NAS)類型產品遭受攻擊，主要為利用漏洞進行攻擊與入侵，影響後果包含設備資料遭勒索加密、使用系統資源進行挖礦及造成資料毀損等。

NAS 產品因其容易操作特性，設置與存取不需要資訊專業人員協助，相較其他資料儲存方式，成本較低且具備橫向擴充彈性，可輕鬆備份資料與存取。根據統計，不論是在一般用戶與企業用戶，對於 NAS 之使用需求皆逐年成長，因此相關攻擊亦漸趨成長。

以下將針對 NAS 之攻擊案例進行分析，並提供相關資安防護建議供參。

2.1 攻擊案例分析

NAS 產品除做為資料儲存用途外，同時也提供各類軟體擴充套件，一旦作業系統本身與應用程式存在可利用漏洞，於設備連網之情況下，即可能遭受攻擊。分析遭鎖定廠牌以聯通科技之 QNAP 為大宗，入侵手法以利用系統漏洞與暴力破解密碼方式為主，詳見圖 4。

惡意程式名稱	目標廠牌	主要影響	入侵手法	CVE編號
AgeLocker	QNAP	勒索軟體	CVE	CVE-2020-2506, CVE-2020-2507
Dovecat	QNAP	挖礦劫持	暴力破解	無
eCh0raix	QNAP	勒索軟體	CVE	CVE-2021-28799
	Synology		暴力破解	無
Qlocker	QNAP	勒索軟體	CVE	CVE-2020-2509, CVE-2020-36195
UnityMiner	QNAP	挖礦劫持	CVE	CVE-2020-2506, CVE-2020-2507
.nttpd,1-ppc-be-t1-z	WD	資料毀損	CVE	CVE-2018-18472, CVE-2021-35941

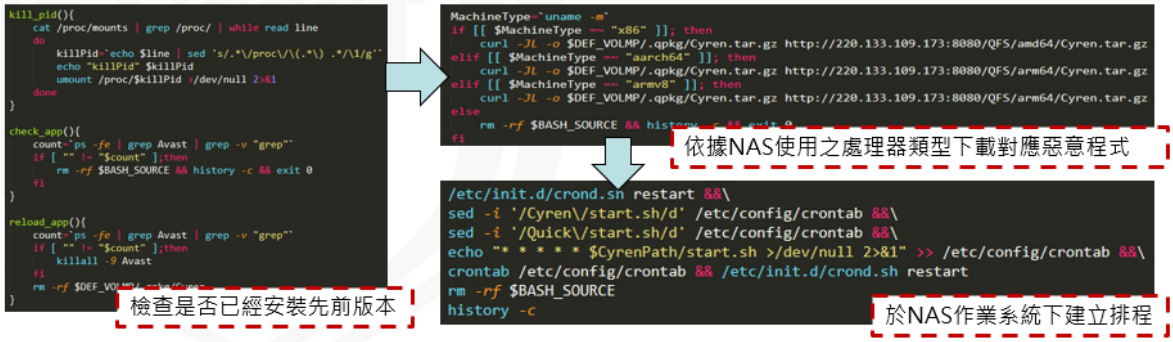
資料來源：本報告整理

圖4　NAS 攻擊案例分析

以 UnityMiner 惡意程式為例，資安廠商於 110 年 3 月揭露，UnityMiner 以 QNAP NAS 做為攻擊目標，成功利用 QNAP NAS 作業系統(QTS)之 Helpdesk

應用程式漏洞(CVE-2020-2506 與 CVE-2020-2507)入侵後，進行挖礦劫持。CVE-2020-2506 為權限控制漏洞，可讓攻擊者取得 QNAP NAS 之控制權限；CVE-2020-2507 為指令注入漏洞，可讓攻擊者遠端執行任意程式碼。若韌體更新日期為 109 年 8 月之前，則有遭攻擊之風險，受到影響型號多達 100 多種。

攻擊者會嘗試利用 QNAP NAS 應用程式漏洞進行攻擊，於成功入侵並取得權限後，對外下載惡意程式腳本並執行，分析其惡意腳本(unity_install.sh)執行流程，詳見圖 5。



資料來源：本報告整理

圖5　惡意腳本分析

進一步分析其挖礦劫持流程，UnityMiner 惡意程式於設備執行上述 unity_install.sh 惡意腳本並下載惡意程式後，會將 start.sh 加入排程並執行挖礦相關行為，包含檢查設備處理器數量，並修改挖礦程式設定檔(config.json)，亦將 NAS 系統路徑下 manaRequest.cgi 原始檔案刪除，並以惡意程式中同名檔案進行置換等。該原始 manaRequest.cgi 檔案，為 NAS 作業系統用於檢查目前設備處理器使用率，而置換過之 manaRequest.cgi 檔案，會竄改相關數據並寫入設備 Log 檔中，使用者將無法從系統管理工具中直接觀察到 NAS 作業系統 CPU 使用率異常，藉此隱匿挖礦劫持行為，詳見圖 6。

資料來源：本報告整理

圖6　竄改數據以隱匿挖礦劫持

分析其連線礦池之連線封包與惡意程式所使用之設定檔，挖礦程式之設定檔中提供 7 組礦池連線 IP:Port，特別是使用 Port:38933 之礦池主機，皆為 QNAP NAS 主機，研判係遭駭客入侵後，安裝相關服務做為礦池，目前對應服務皆已停止。

2.2 政府骨幹偵測與防護作為

分析政府骨幹流量觸發挖礦偵測規則狀況，依據 110 年已發布 INT 警訊與機關通報內容進行分析，共計 6 筆警訊為 NAS 遭挖礦劫持。5 個機關為 QNAP NAS 遭植入 UnityMiner 惡意程式，另 1 個機關為 Synology NAS 因弱密碼遭入侵後被植入挖礦程式。清查時發現政府骨幹上可能遭受 UnityMiner 惡意程式影響之 QNAP NAS 型號，尚有 2 台未更新至 109 年 8 月 17 日所釋出之韌體版本，已即時發送資安預警警訊，通知設備所屬機關因應處置。

現今不論是一般用戶或企業用戶，對於 NAS 之使用需求皆逐年成長。因此，相關資安防護作為更應謹慎因應，特別是 UnityMiner 會隱藏挖礦進度與記憶體資源使用率以規避偵測，不利早期發現。從攻擊案例分析得知，作業系

統韌體更新是最基本且易被忽視項目，應積極設定為自動更新，詳見圖 7。

資料來源：本報告整理

圖7　韌體自動更新

同時檢視應用程式自動更新機制，除應用程式版本更新與管理外，亦應定期審視已安裝之套件/應用軟體之適切性。若評估已無使用需求之服務，應儘速停用或移除，以降低弱點遭利用之資安風險。

另外，應針對存取權限加強控管，評估連網設備相關風險，考量使用狀況限縮存取權限與範圍。同時，訂定使用者帳號密碼設定與審視管理機制，密碼設定除應符合密碼複雜度原則、定期更改密碼及定期審視有無未知或可疑帳戶外，建議亦須停用預設管理者帳號，改採新增帳號至 admin group 方式處理。

許多外部嘗試登入帳號名稱多使用包含 administrator, admin 及 root 等，可見預設帳號留存為高風險之管理行為，建議啟用自動封鎖功能，因外部嘗試登入設備方式，多採用自動化工具進行，可透過啟用帳號保護與自動封鎖功能，降低對帳號進行暴力破解攻擊之風險。最後，應避免使用預設管理連接埠，變更 NAS 管理頁面之預設連接埠，以降低駭客使用自動化工具進行攻擊之可能性。

3.資安技術研析_Mozz 殭屍網路攻擊案例分析

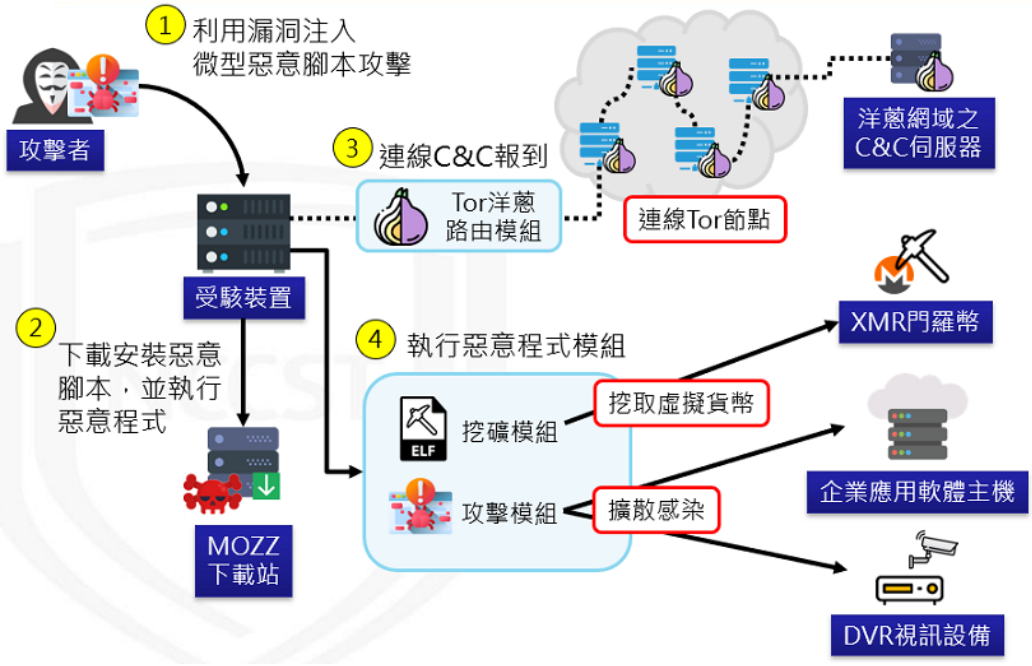
本季探討之資安技術研析為 Mozz 殭屍網路攻擊案例分析，技服中心於 110 年 9 月初發現 Mozz 殭屍網路使用企業應用軟體與視訊設備(Digital Video Recorder, DVR)之漏洞進行攻擊與擴散感染。透過蜜罐(honeypot)系統成功捕獲 Mozz 殭屍網路，揭露其針對開源內容管理系統 Drupal 之漏洞進行攻擊，注入微型惡意腳本等行為。受駭主機將連線至下載站，順利取得安裝惡意腳本，下載安裝惡意程式 ntpclient，以進行擴散感染與挖礦行為。

Mozz 殭屍網路除利用內容管理系統包含 Drupal 與 Confluence 之軟體漏洞，成功展開攻擊外，尚利用企業資源規劃軟體 InoERP 與 IT 軟體如 Hadoop YARN 及 mongo-express 等。藉由攻擊偵測分析發現 DVR 也為殭屍網路攻擊目標，包含歐洲品牌 Visual Tools 與中國海康威視之漏洞皆曾被揭露使用。

以下將針對 Mozz 殭屍網路攻擊進行說明，並概述攻擊趨勢與防護作為。

3.1 惡意程式與下載檔案分析

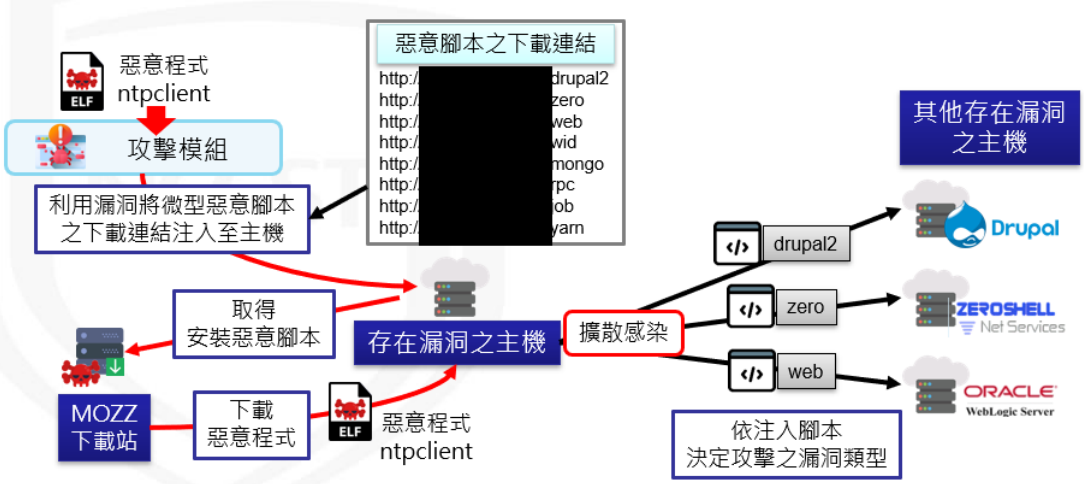
Mozz 殭屍網路程式包含 13 種漏洞攻擊工具，主要利用現有系統與設備漏洞入侵，攻擊流程與目標對象詳見圖 8。



資料來源：本報告整理

圖8　攻擊流程與目標對象

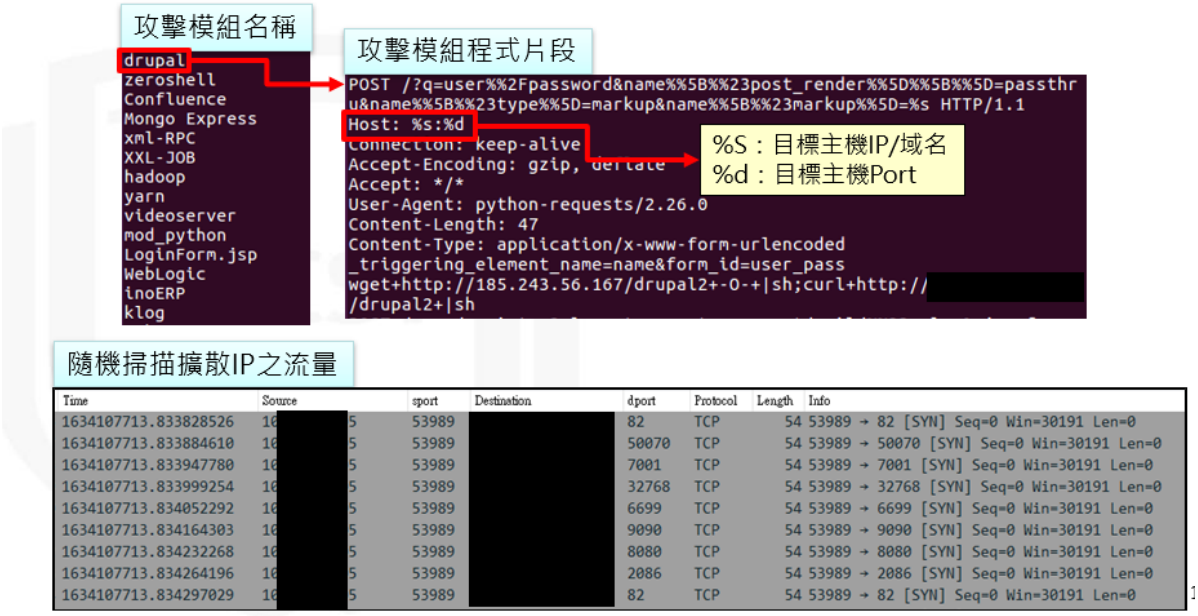
分析惡意程式 ntpclient，發現 8 個安裝惡意腳本下載連結，可供漏洞攻擊模組注入微型惡意腳本至受駭主機使用。各腳本分別用於擴散感染各種軟體之漏洞，如 Drupal、Zeroshell 及 Weblogic 等系統，詳見圖 9。



資料來源：本報告整理

圖9　惡意腳本下載

分析惡意程式過程中，發現 ntpclient 惡意程式為阻止被反編譯破解已採取加殼動作，因此需再脫殼進行分析。同時也解析此惡意程式啟動後，會刪除主機相關競爭程式，以利後續動作。此外，ntpclient 惡意程式帶有多個漏洞攻擊模組，會隨機產生目標 IP 以進行擴散攻擊，詳見圖 10。

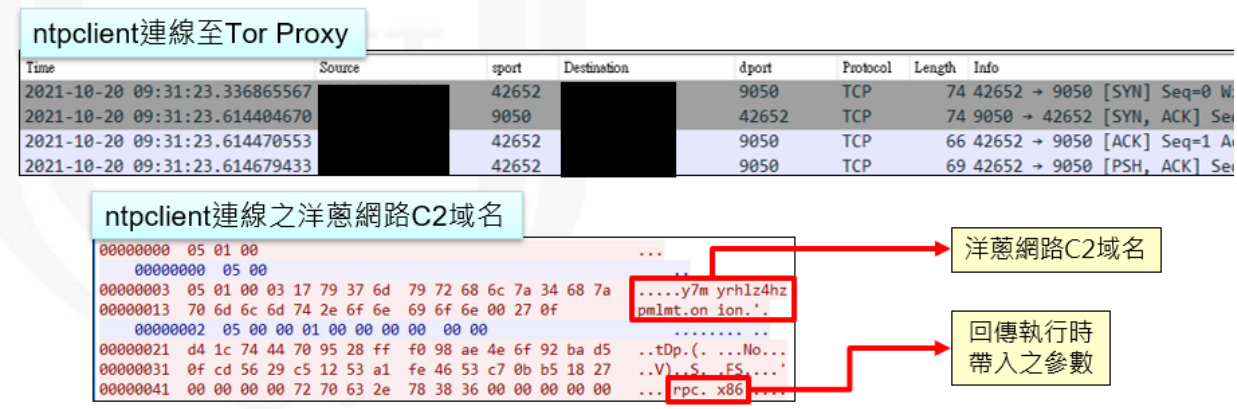


資料來源：本報告整理

圖10 隨機擴散攻擊

ntpclient 惡意程式包含 XMRig 開源之挖礦程式片段，程式生成礦池與錢包等資訊之設定檔，供 XMRig 挖礦模組使用。俟 ntpclient 惡意程式成功感染主機後，會以隨機產生名稱之程序啟動挖礦行為，並占用主機大量 CPU 資源。

另外，ntpclient 惡意程式亦可使用洋蔥網路(Tor)連線 C2 進行惡意活動，以 XOR 0x65 為金鑰解碼，可解出洋蔥網路 C2 之域名，後續再透過隨機選取之 Tor Proxy(Port 9050)連線洋蔥網路 C2 域名，詳見圖 11。

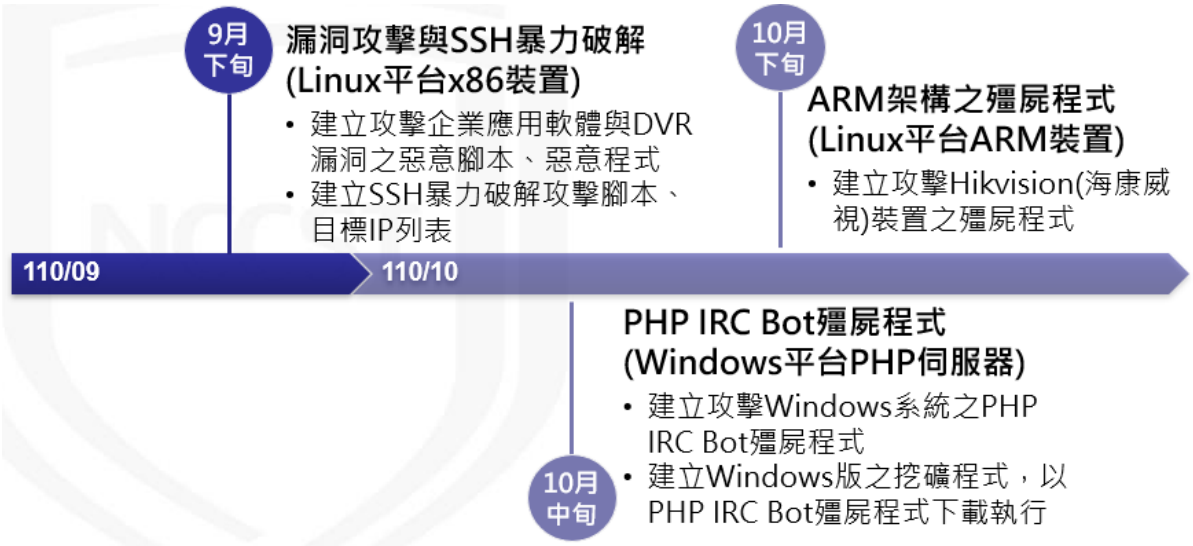


資料來源：本報告整理

圖11 Tor 連線 C2

3.2 攻擊偵測分析

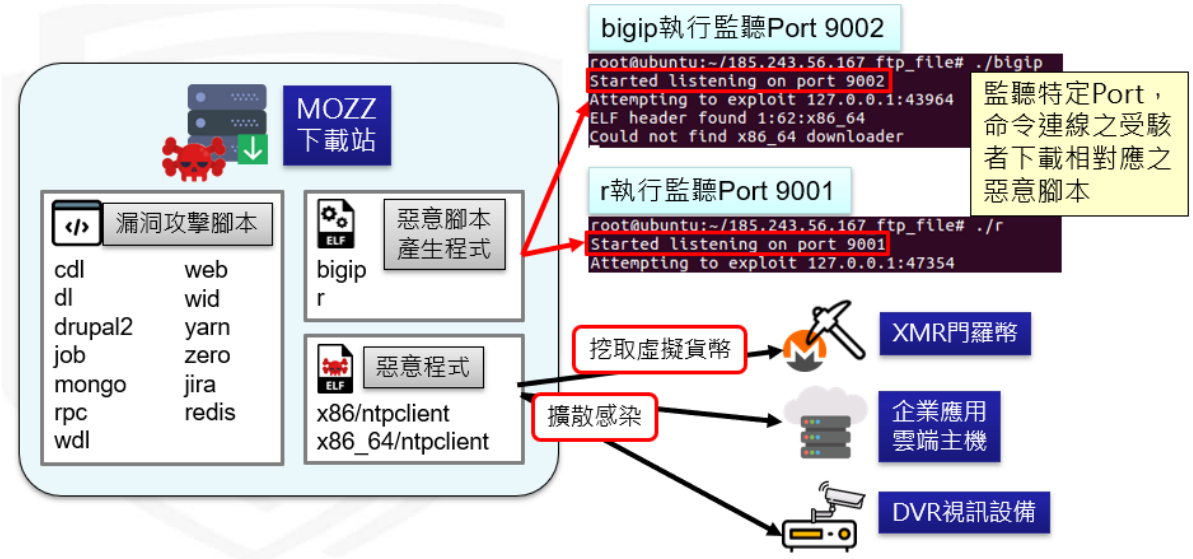
偵測發現駭客建立之下載站，於 110 年 9 月~10 月期間陸續新增攻擊之腳本、惡意程式及駭客工具，藉以擴增攻擊裝置類型，詳見圖 12。



資料來源：本報告整理

圖12 Mozz 殭屍網路攻擊偵測

110 年 9 月下旬新增之檔案，主要為針對企業應用軟體與 DVR 設備之漏洞攻擊腳本、惡意程式及惡意腳本產生程式，詳見圖 13。



資料來源：本報告整理

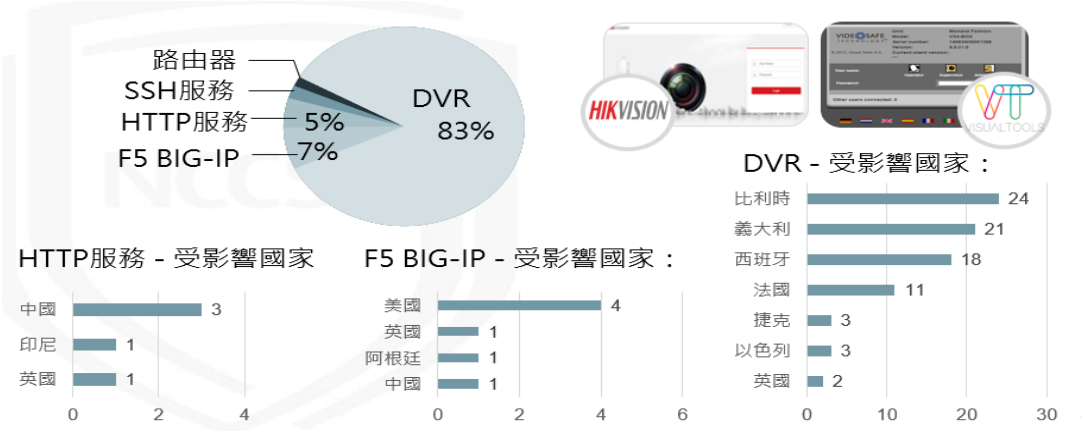
圖13 漏洞攻擊腳本與程式

另一波攻擊則為 SSH 暴力破解用途之相關檔案，駭客建立 SSH 攻擊目標之 IP 列表與 SSH 攻擊腳本，再以此腳本啟動 ntpclient 惡意程式。

接續於 10 月中旬新增 PHP IRC Bot 殭屍程式、挖礦程式及駭客工具，以 Windows 平台 PHP 伺服器為攻擊目標，因 PHP IRC Bot 殭屍程式已有公開原始碼，駭客則依需求自行修改程式，新增下載挖礦程式之功能，分別使用駭客工具，包含 netcat 與 powercat 用於入侵與滲透之用途。PHP IRC Bot 程式碼因已設定下載站為 IRC 伺服器，PHP IRC Bot 成功植入攻擊目標後，可遠端接收指令，其功能包含遠端執行系統指令、下載檔案及發動阻斷服務(Distributed of Service, DoS)攻擊等功能。駭客得以自行修改程式，新增下載挖礦程式之功能，以 PowerShell 與 PHP 指令等 2 種方法下載執行挖礦程式。

而另一波攻擊則為 ARM 架構之殭屍程式，對象為 Linux 平台 ARM 設備，駭客新增建立攻擊 Hikvision(海康威視)裝置之殭屍程式，此殭屍程式之程式片段與 110 年 9 月下旬惡意程式 ntpclient 相同，目的為藉以擴充殭屍網路之攻擊裝置範圍。

Mozz 殭屍網路攻擊漏洞大多以企業軟體為主，而 DVR 受駭數量相較多數，推測可能與 DVR 韌體更新支援較少有關。分析受駭裝置與受駭國家統計，詳見圖 14。



資料來源：本報告整理

圖14 受駭裝置與國家

進一步分析受駭裝置之網際網路連線服務公司(Internet Service Provider, ISP)主要為一般電信業者，來源國家以歐洲居多，受駭裝置除 DVR 視訊設備外，其他亦包含少量一般網站、路由器、F5 BIG-IP。其餘 ISP 為雲端服務(如微軟 Azure 與阿里雲等)，受駭服務包含 F5 BIG-IP、Portainer 及 Mongo 等服務。

整體而言，Mozz 殭屍網路，主要攻擊目標為企業雲端服務與 IoT 設備，並持續擴散感染做為虛擬貨幣挖礦之用途。因此，建議企業使用雲端服務與 DVR 設備時，除嚴謹控管憑證安全、設定與監控相關服務應用存取，針對 IoT 設備啟用時應立即變更預設密碼外，亦應定期且即時更新版本修補漏洞，以確保主機安全。技服中心亦已依所掌握之情資對受駭單位發布警訊，並透過 N-ISAC 分享情資，供受駭機關與國家能即時處理，後續將持續追蹤，以強化資安防護能量。

4. 結論

本季具指標性案例為重大漏洞 Log4Shell 攻擊態勢加劇，陸續傳出攻擊者開始利用該漏洞展開各種攻擊之事件，如安裝加密挖礦程式、竊取系統憑證及竊取資料等。相關攻擊擴展至各項知名網路服務、國防單位及工控系統，影響甚鉅。第 2 起案例為殭屍網路惡意程式利用老舊漏洞，攻擊 IoT 裝置。資安實驗室 Alien Labs 揭露新殭屍網路惡意程式 BotenaGo，利用已知之老舊資安漏洞，鎖定逾百萬台 IoT 設備展開攻擊行動。

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「IoT 之資安管理」、「個資遮蔽與保護之資安管理」及「組態設定與系統變更之資安管理」提出資安防護建議。

資安專題分享主題為 NAS 相關產品遭受攻擊與影響後果，攻擊者利用其應用程式漏洞進行攻擊，於成功入侵並取得權限後，對外下載惡意程式腳本並執行。特別是惡意程式會隱藏挖礦進度與記憶體資源使用率以規避偵測，不利早期發現，為防患於未然，本報告亦針對 NAS 相關產品之防護措施提出建議。

另外，資安技術研析主題為 Mozz 殭屍網路攻擊案例分析，發現 Mozz 殭屍網路使用企業應用軟體與視訊設備之漏洞進行攻擊與擴散，主要針對開源內容管理系統 Drupal 之漏洞進行攻擊。藉由攻擊偵測分析發現 DVR 亦為殭屍網路攻擊目標，技服中心已依所掌握之情資對受駭單位發布警訊，並透過 N-ISAC 分享情資，供受駭機關與國家能即時處理。

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：

◆ 跨國攻防演練 CODE 2021

行政院國家資通安全會報每 2 年辦理 1 次大規模跨國攻防演練(Cyber Offensive and Defensive Exercise, CODE)，110 年辦理日期自 11 月 16 日至 11 月 18 日止，期藉由攻防演練檢視關鍵基礎設施提供者之通報應變作業與資安防護完備度，並於活動期間邀請國內外專家參與實際攻防與經驗交流分享。

此次以能源領域做為模擬演練場域，邀請國內外資安攻擊好手與能源公司進行紅藍隊即時對抗，以模擬煉油廠工控設施可能遭受攻擊之途徑，以及受到攻擊時之偵測與通報應變處理措施，進行紅藍對抗實兵演練。於攻防演練活動後，安排研討會就紅藍對抗攻防演練結果與各國訪賓進行實務研討，期透過本次演練與參與人員進行經驗分享及共同學習成長，提升彼此資安攻防技術與應變能力，進而促進跨國聯防與深化國際合作。

◆ 行政院國家資通安全會報第 38 次委員會議(擴大會議)

行政院國家資通安全會報第 38 次委員會議於 110 年 12 月 7 日假台大醫院國際會議中心辦理，分上下午場次。會議上午場次主題分別有「教育體系資安強化策略」、「資安經驗分享與建議」、「資安推動策略及重要工作」及「數位政府基礎環境之資源整合策略」等主題。討論項目包含教育體系之整體資安督導架構與全面落實資安之作業規劃，藉由公私不同產業之資安經驗與分享，促進不同面向之管理流程與技術作業之持續精進。資安推動策略敘及資安推動之重要工作，包含內部應原則禁止遠端連線、導入資安弱點通報及端點偵測機制等配合事項。數位政府基礎環境之資源整合策略，除強調資安專責人力補足之重要性，同時要求落實資安集中防護，避免資源重覆投入。

會議下午場次聚焦於 111 年度資安重點工作及配合事項，包含確認國家資通安全發展方案(110 年至 113 年)各項具體措施之達成情形與規劃應處作為、資通安全管理法子法修正條文配合事項與相關資安配合事項，如定期填報大陸廠牌資通訊產品清冊、落實視訊會議及即時通訊軟體使用安全等。另外，說明資安採購及聯合稽核重點，如即時揭露系統資安防護等級、資安經費及定期對委外廠商辦理稽核等。