112年第3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 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。

●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 AI 網路犯罪工具，遭駭客運用於網路釣魚與惡意程式攻擊；另一案例為駭客使用新版 Sphynx 變種展開攻擊行動，加密受駭系統與遠端 Azure 雲端儲存體。

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 50.18%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 9.687%)與「網頁攻擊」(占 7.89%)為主要通報類型。

●資安專題分享

資安專題分享主題為 QR Code 網路釣魚攻擊，隨著 QR Code 普及，出現許多以電子郵件寄送 Quishing 入侵案例，駭客利用電子郵件內插入惡意 QR Code 圖片或圖片連結，偵測機制可能無法察覺 QR Code 內含之惡意網址與若使用者透過行動裝置連線，將無法即時辨識，可成功規避資安防禦機制之偵測。

●資安技術研析

資安技術研析主題為 AndoryuBot 新型殭屍網路研析，資安業者揭露 AndoryuBot 新型變種，此新型變種攻擊鎖定多個 Ruckus 無線產品為攻擊目標，將感染後操縱為 AndoryuBot 殭屍網路，藉以發動分散式阻斷服務攻擊。

●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 QR Code 網路釣魚攻擊，駭客積極研析以 QR Code 攻擊之可行性，藉由相關案例分享，說明因應此類攻擊之檢測機制與防護建議。此外，資安技術研析分析為 AndoryuBot 新型殭屍網路研析，研究發現駭客除持續利用該漏洞擴散殭屍網路，且發起各種協定之 DDoS 攻擊外，同時公開行銷 DDoS 攻擊服務，應持續隨時關注此駭客族群之樣態。

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。112 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。

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

網路威脅與非法事件，一直是犯罪活動中持續成長產業之一。隨著此類黑色產業鏈之經濟規模日益擴張，因其分工與與功能精緻化，對產業造成之經濟衝擊亦顯著加劇。黑色產業鏈不僅分工明確，藉由網路犯罪即服務之快速攻擊服務模式，讓網路攻擊事件屢見不鮮。

而隨著人工智慧(Artificial Intelligence, AI)興起，一個很明顯的案例是聊天機器人助長社交工程詐騙更加擬真化。藉由非法蒐集之個人資訊，再輔以人工智慧之聊天機器人模擬真實資通服務，讓缺乏資安意識之使用者更容易上當受騙，且由於現今許多組織提供線上客戶服務系統，亦讓使用者習慣相關介面，而疏忽辨識真偽。

本季具指標性案例為 AI 網路犯罪工具，遭駭客運用於網路釣魚與惡意程式攻擊；另一起案例為駭客使用新版 Sphynx 變種展開攻擊行動，加密受駭系統與遠端 Azure 雲端儲存體。

首先，探討案例為資安業者 SlashNext 揭露駭侵者於暗網與社群媒體平台積極推銷 AI 網路犯罪惡意程式 WormGPT 與 FraudGPT，讓購買者可以輕易使用工具展開網路釣魚攻擊活動。SlashNext 先報導 WormGPT 之出現，其創造者宣稱此工具為利用 OpenAI 開發之人工智慧聊天機器人，可以模擬人類思維設計詐騙訊息，例如，此聊天機器人能仿真設計看起來信賴可

靠之訊息，模仿合作夥伴支付款項或變更交易事項等，該軟體開發最大目的應為發展網路釣魚電子郵件與商業電子郵件外洩攻擊。

陸續又於市場上發現另一 AI 網路犯罪惡意程式 FraudGPT，另一資安業者 Netenrich 揭露於暗網上有註冊使用者名稱為 CanadianKingpin12 於暗網與社群平台鎖定網路詐騙者、駭客及垃圾郵件寄送業者，行銷其 AI 網路犯罪惡意程式。從其展示之功能可發現，AI 網路犯罪惡意程式提供數項功能，包含提供零時差攻擊弱點、協助執行進階社交工程攻擊以操控個人、揭露一般與關鍵基礎設施等資通系統弱點、提供與創造惡意程式，特別是針對勒索軟體之攻擊、能提供設計與發展複雜之網路釣魚活動。

訂閱這些 AI 網路犯罪惡意程式服務之使用者，即能藉由所提供之惡意程式碼、網路釣魚網頁、駭客攻擊工具及系統漏洞，讓訂閱者可以輕易發動攻擊。這些 AI 網路犯罪惡意程式甚至還會協助尋找具代表或指標性之服務網站，以便精準地詐騙更多使用者，而從其銷售頁面可得知避免被偵測或潛藏軌跡亦是功能選項之一。此外，另一個針對 AI 網路犯罪惡意程式發展趨勢為這些工具之開發人員基於便利性原則，會提供應用程式介面 (Application Programming Interface, API)存取，以簡化工具整合至惡意使用者之作業流程與程式碼過程，預料將使這類攻擊案例大幅上升。

第 2 起案例為微軟雲軟服務平台 Azure 遭勒索團體入侵，並加密資料。駭客族群 BlackCat，又名為 ALPHV，使用外洩之微軟使用者帳號，再用最新發表之 Sphynx 加密器，加密遭鎖定之 Azure 雲端儲存體。

資安業者 Sophos 在調查最近一件資安事件時發現入侵者使用新版 Sphynx 變種展開攻擊行動，加密受駭系統與遠端 Azure 雲端儲存體。駭客藉由使用遭竊之一次性密碼 (One Time Password, OTP)，獲取管理產品之存取中控台 Sophos Central 帳戶存取權限後，系統隨即遭停用防篡改功能並修改安全性原則。據推測分析遭竊之 OTP 可能來自於受害者使用 LastPass

Chrome 已儲存密碼之自動登入功能而外洩。入侵手法為將攻擊之金鑰使用 Base64 編碼後注入勒索軟體二進位檔案，並在所有所有被加密檔案中新增新增.zk09cvt 副檔名，總計加密 39 個 Azure 帳號之儲存體。

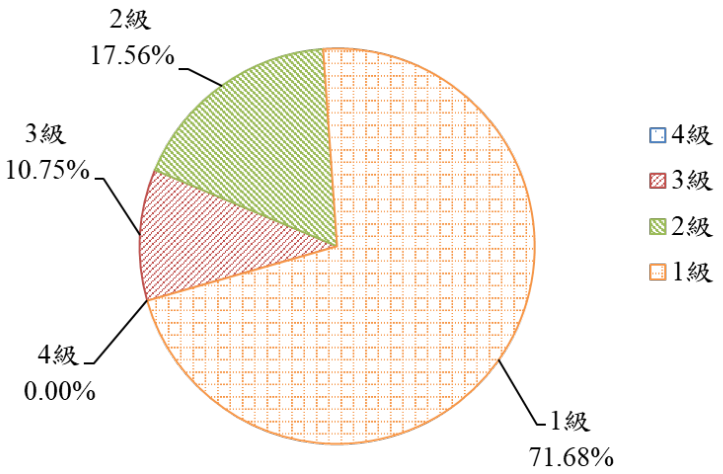
而駭客為繼續操控該系統，持續利用 AnyDesk、Atera、Splashtop 及其他遠端監控與管理工具。除相關遠端監控與管理工具外，亦發現駭客為加速資料竊取速度，同時使用 Exmatter 資料竊密工具，猜測目的應為在加密資料前，能先快速將資料傳送到駭客指定之伺服器。特別需注意重點為新版 Sphynx 變種包含利用 Impacket 網路框架與 Remcom 駭客工具等，以進行憑證複製與遠端服務執行命令，目的為加強其橫向擴散能力。同時，此駭客族群更在其新版勒索軟體加入資料外洩應用程式介面(Application Programming Interface, API)，亦顯現駭客入侵後企圖利用各種方式，提高攻擊能見度且造成重大衝擊後，達到其勒索目的。從此次新版 Sphynx 變種攻擊案例可得知，BlackCat 已成功發展出成熟勒索軟體攻擊用之工具包，將可更快在受駭系統上部署加密行動。

綜覽本季全球資安威脅與資安事件，人工智慧尤如雙面刃，可以協助於大量資安事件或日誌中，快速學習與發展偵測技術，另一方面，藉由 AI 技術所發展之網路犯罪工具，亦日漸猖獗。而且隨著駭客族群持續發展新式變種攻擊技術之際，網路攻擊之風險亦持續升溫，因此建立全面與時俱進之資安思維與防護策略，有助於因應接踵而來之複雜且變化攻擊，提升維運韌性。

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」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

71.68%為大宗，2 級事件占 17.56%次之，3 級事件僅占 10.75%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

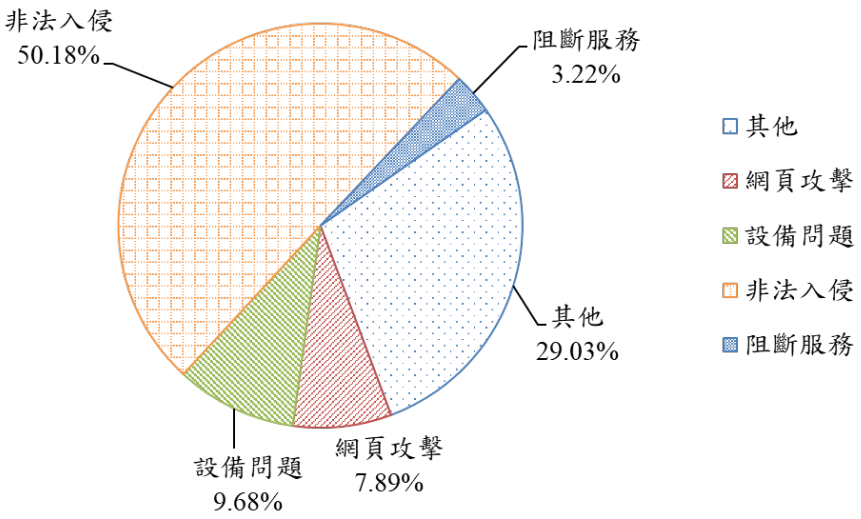


資料來源：本報告整理

圖1　112 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，有某機關發現電子郵件系統存在驗證機制失效風險。因曾設定郵件系統可透過 AD 或本機同步驗證登入資訊，後續雖已關閉同步設定，惟未能清除本機資料，造成舊版密碼仍可登入之問題，於第一時間偵測到疑似遭駭客利用異常登入存取行為。另一事件為發現有政府機關之數位監視系統因連線組態設定關係公開於網際網路，包含通訊埠連線介面與網頁登入介面，因此存在介面暴露，可能允許外部使用者進行惡意之掃描刺探，致遭入侵攻擊之風險。

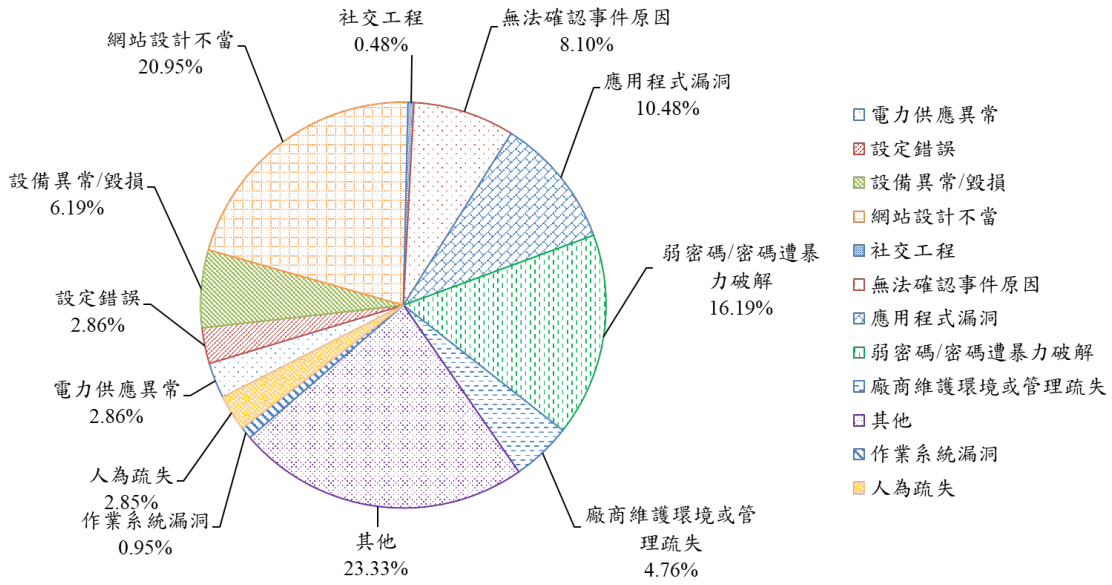
整體通報事件類型，以「非法入侵」(占 50.18%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



資料來源：本報告整理

圖2　112 年第 3 季通報類型比率圖

分析通報事件發生原因，可發現事件原因以其他(23.33%)為主，其次分別為網站設計不當(20.95%)、弱密碼/密碼遭暴力破解(16.19%)、應用程式漏洞(10.48 %)、無法確認事件原因(8.10%)、設備異常/毀損(6.19%)、廠商維護環境或管理疏失(4.76 %)、設定錯誤(2.86%)、電力供應異常(2.86 %)、人為疏失(2.85 %)、作業系統漏洞(0.95%)及社交工程(0.48 %)，詳見圖 3。



資料來源：本報告整理

圖3　112 年第 3 季資安事件發生原因比例圖

分析第 3 季通報類型與通報事件發生原因，本季無法確認事件原因包含機關發生系統短暫異常，經重啟後即恢復正常或機關調查錯誤訊息紀錄與系統資源消耗後，尚無法釐清異常原因。其他之案例，則有使用者下載或安裝來源不明之應用程式與套件等或或連線數超過系統負荷以致系統資源不足影響正常營運。綜整網站設計不當之資安事件，包含設計網頁存在漏洞、未限制檔案上傳及不當的存取控制，致取得活動民眾申請或報名結果之網址連結，即可查看該個人之所有資料；弱密碼或密碼遭暴力破解占 16.19%，從事件分析中得知，除使用預設密碼或弱密碼致入侵成功外，讓惡意程式得以快速橫向擴散之原因為相關資訊設備設置相同帳號密碼，導致某案例被遭勒索軟體攻擊成功，造成多台資訊設備檔案被加密，致資通服務中斷。

1.3 資安防護重點

分析本季全球資安威脅現況，駭客使用 AI 網路犯罪工具，預見未來 AI 工具將成為網路詐騙與攻擊氾濫之利器，再加上黑色產業鏈之影響，此類工

具恐更加唾手可得，因此加強 AI 網路犯罪模式因應之教育訓練與技術偵測更應加快腳步，防患於未然。憑證或密碼機制之失效，常形成可能威脅，使用預設密碼、弱密碼或已儲存之密碼，皆有可能造成身分認證機制失效之後果，特別是因便利性而使用記憶密碼自動登入，更加添憑證外洩之風險。

國內部分發現數位監視系統因連線組態設定關係公開於網際網路，可能允許外部使用者進行惡意之掃描刺探，存在遭入侵攻擊之風險。且因管理者普遍對數位監視系統管理嚴謹度較低，常發生密碼未變更或使用弱密碼等狀況，從已偵測之資安事件中分析，多為密碼遭破解，而為入侵者成功遠端登入並操控系統。

綜整以上資安威脅現況，提供資安防護建議如下：

●AI 網路犯罪工具之資安管理

– 提供與時俱進之資安教育訓練，教育使用者了解新興攻擊之方式與因應策略。

– 強化訊息接收之技術驗證，例如：加強電子郵件驗證措施，且採取嚴謹之過濾與關鍵字篩選原則。

– 建立惡意流量偵測機制，透過 AI 研究分析已知惡意程式的網路行為特徵與模式，快速偵測與分析異常網路流量。

●數位監視系統之資安管理

– 依內部風險管理與資安政策，訂定資訊設備內外部存取策略，非必要，應設定於非對外公開網路區域。

– 資安健診活動應涵蓋數位監視系統系統操控程式之應用程式介面，定期測試系統漏洞與修補更新活動。

– 設定強密碼，非必要之帳號應刪除或停用；檢視資通設備與資安防護設備之日誌，偵測系統異常行為。

2. 資安專題分享_QR Code 網路釣魚攻擊

資安業者 Cofense 從本年 5 月開始觀測到大量利用電子郵件散播偽冒之微軟安全性通知，要求掃描二維條碼(Quick Response Code, QR Code)進行微軟憑證驗證之網路釣魚活動。主要目標對象為一家美國大型能源公司，屬於關鍵基礎設施產業，分析發現於千餘封郵件中，約有 29%電子郵件內嵌惡意二維條碼，攻擊目標尚含製造業、保險業、科技業及金融服務業等，從這波攻擊活動資安業者亦揣測駭客可能正在研析以 QR Code 攻擊之可行性。

從另一資安業者 Zscaler 於其 ThreatLabz 2023 Phishing Report 中指出，與 111 年相比，釣魚郵件攻擊劇增 47.2%，且有持續上升之趨勢，而駭客為能一舉發動大規模之攻擊活動，其入侵手法亦不斷翻新。分析網路釣魚攻擊事件中，發現隨著 QR Code 因運用於各樣資通服務上之快速成長，亦衍生出大量 QR Code 網路釣魚攻擊。因此除宣導與加強防範此類新興威脅之案例與手法外，後續仍需持續觀測此類新興威脅之擴展與變化。

以下將概述 QR Code 網路釣魚攻擊手法與威脅，藉由相關案例，說明因應此類攻擊之檢測機制與防護建議。

2.1 釣魚攻擊手法概敘

現今網路釣魚攻擊已有多種樣態，依攻擊目標與傳遞管道之不同，大致可分類為幾種較風行之網路釣魚攻擊類型，以目標導向之網路釣魚類型則有不分對象之 Common Phishing，另外有具針對性之 Spear Phishing 魚叉式網路釣魚，為事先已蒐集特定人士之相關資料，針對目標對象發送訊息，與一般制式詐騙訊息相比，訊息因經過關聯性設計，更加具服說服力；與魚叉式網路釣魚有異曲同工之妙者有 Whaling 捕鯨網路釣魚，同樣鎖定特定目標，惟顧名思義 Whaling 攻擊主要鎖定高階管理階層，例如假冒主管要求員工執行交辦事項。

若以傳遞管道區分，則有聲音釣魚(Vishing)，透過聲音方式詐騙使用者；簡訊釣魚(Smishing)為運用手機文字簡訊之網路釣魚攻擊手法；詐騙釣魚(Deceptive Phishing)乃偽冒為一家真實存在之公司，知名詐騙範例為偽冒相似域名與告知所鎖定目標，要求重新認證等不實訊息；二維條碼釣魚(Quishing)則為 QR Code Phishing，為近年新增之網路釣魚類型，隨著 QR Code 應用普及，出現許多以電子郵件寄送 Quishing 入侵案例。因 QR Code 本身為圖像檔案，部分防護機制無法偵測圖像檔案之連結是否為惡意，使這類型釣魚詐騙成功案例大幅篡升。且 Quishing 利用受騙人員慣於使用個人行動裝置掃描 QR Code，當透過行動裝置網路連線至駭客架設之伺服器後，即脫離內部網路安全控管與追蹤機制，如此亦增加後續辨識與追蹤入侵來源之困難度。

分析 Quishing 逐漸流行之原因，從 QR Code 被創造出來後，相較於一維條碼，QR Code 能存放更多資訊，包含文字、數字及 URL 等，並依儲存容量、大小及除錯級別等，發展出各式 QR Code 類型應用。例如，隨著人工智慧發展，創造出以人工智慧生成之圖像，並嵌入 QR Code 提供智慧手機掃描，預料將更大受歡迎，蔚為風潮同時，亦提供有心人士有機可趁之可能性。

進一步了解駭客喜歡使用 Quishing 釣魚，另一原因應為規避資安防禦機制之偵測，主要原因為於電子郵件內插入惡意 QR Code 圖片或圖片連結，一般偵測機制無法直接取得 QR Code 內含之網址，且若使用者透過行動裝置連線，將可成功躲避網路安全偵測機制，分析二者攻擊手法，詳見表 1。

表1　釣魚攻擊手法比較

	一般釣魚郵件(Phishing)	QR Code 釣魚郵件 (Quishing)
惡意連結嵌入手法	於內文插入釣魚連結(URL)	於內文插入惡意 QR Code 圖片或圖片連結
觸發平台	個人電腦	個人行動裝置
偵測機制	入侵防禦/偵測系統/沙箱(IPS/IDS/Sandbox)可直接偵測 URL	不易偵測圖片與合法下載網站連結 手機連線可躲避網路安全偵測機制

資料來源：本報告整理

以下接續說明 Quishing 攻擊樣態，包含架設偽冒合法網站與惡意 APP，分析 Quishing 惡意郵件主旨案例，同時提供可行之防護建議。

2.2 QR Code 網路釣魚攻擊案例與防護建議

惡意 Quishing 樣態常見形式為架設偽冒合法網站登入頁面之釣魚網站，同時生成釣魚網站 QR Code，駭客會伺機寄發社交工程郵件，當使用者掃描惡意 QR Code 時，即會連線釣魚網站進行騙取個資之動作。另一種常見樣態則為開發惡意 APP 與架設下載頁面，另生成下載頁面之 QR Code，當使用者掃描惡意 QR Code 時，則會連線至惡意 APP 下載頁面，主要目的為誘導下載惡意 APP。

統計分析常見 Quishing 主旨樣態，蒐集且觀測目前已知利用 Quishing 手法之郵件，其主旨樣態之共通模式有時事相關、憑證更新需求等，且皆試圖傳達急迫感，要求收件人迅速採取對應之行動，致使用者無法於第一時間審慎思考，Quishing 主旨樣態可概分為以下種類，詳見表 2。

表2　Quishing 郵件主旨樣態統計

項目	郵件主旨樣態
1	雙因子驗證設定
2	帳戶驗證
3	密碼更新
4	安全性更新
5	電子郵件正在信箱中等待
6	補貼金額申請通知

資料來源：本報告整理

分析 Quishing 社交工程郵件真實攻擊案例，國外案例可見駭客偽冒網路服務公司以「雙因子驗證設定」郵件主旨，誘騙使用者掃描惡意 QR Code 後輸入密碼；另一案例為駭客寄送雲端文件分享通知郵件，誘騙使用者掃描惡意 QR Code 後登入連線至偽冒雲端文件服務登入頁面之釣魚網站。

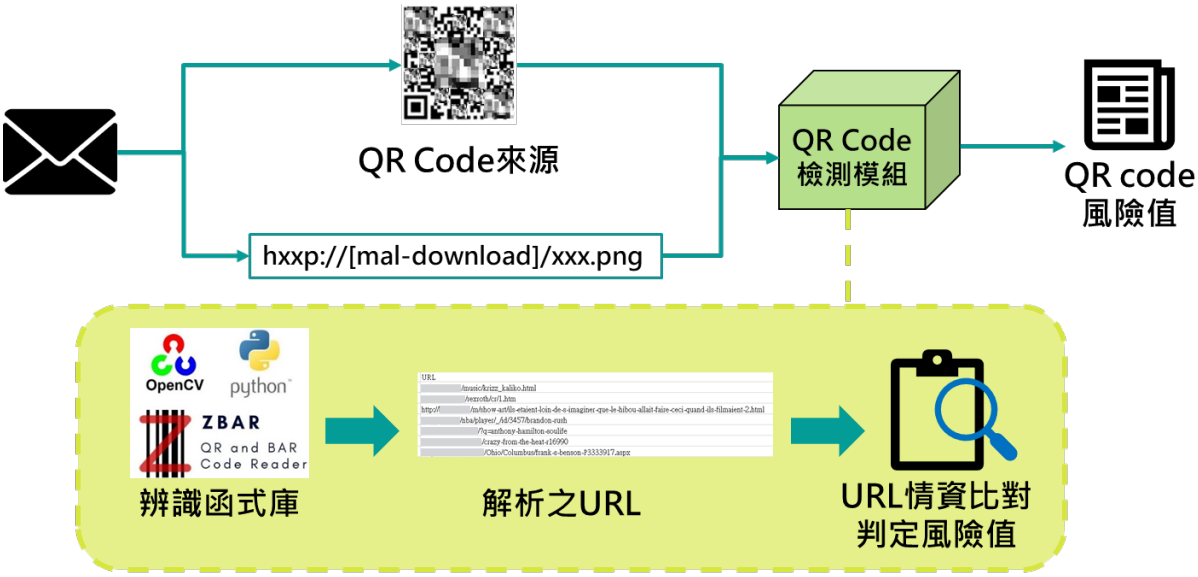
而國內案例中，偵測發現駭客偽冒相似政府機關之郵件帳號，以使用「智慧手機系統上線」為主旨，對機關發動魚叉式社交工程電子郵件攻擊，於郵件中提供教學步驟以要求使用者掃描 QR Code，俟成功誘騙機關人員掃描 QR Code 後，要求輸入郵件帳號密碼。分析郵件內容，發現末端還潛藏追蹤像素(Tracking Pixel)，能回傳開啟該封郵件之 IP 位址至駭客所架設之雲端服務伺服器，追蹤且記錄開啟郵件之相關行為資訊，詳見圖 4。

資料來源：本報告整理

圖4　回傳紀錄至惡意雲端伺服器

面對網路釣魚詭譎多變之攻擊方式，基本防禦機制為先透過設定郵件伺服器之過濾機制，例如：以郵件寄件者、IP 位址或字串等篩選，或網路服務過濾器等阻斷。以政府機關為例，現行部署於機關之惡意電郵檢測機制，主要透過動態沙箱進行行為檢測，若發現惡意電子郵件，則移至隔離區再行檢測，且就威脅情資進行可疑之 URL、IP 及域名比對，可成功防堵一般網路釣魚手法入侵。

但面對已知 Quishing 於郵件內文嵌入圖片、郵件內文嵌入圖片連結或附檔文件嵌入圖片等攻擊手法，則建議郵件檢測機制應透過 OpenCV 視覺化機制與 ZBAR(Bar Code Reader)條碼讀取函式庫等工具建立 QR Code 檢測模組，強化郵件自動化檢測機制，詳見圖 5。



資料來源：本報告整理

圖5　郵件自動化檢測機制

藉由 OpenCV 與 ZBAR 等開源軟體建立辨識函式庫，用於辨識 QR Code 圖像與解析連結之 URL 後，再透過 QR Code 檢測模組判定風險，以強化面對 Quishing 入侵於現有基礎過濾機制不足之處。

雖可依賴技術檢測，減緩網路釣魚之風險，惟因駭客攻擊策略不斷翻新，教育使用者如何檢測惡意之網路釣魚入侵手法，並即時做出做好回應，仍為最佳解決之道。例如：可建議使用可顯示連線網址之 QR Code 掃描工具，以確認網址之正確性。因駭客經常使用前綴為正常機關域名之相似域名，再加上手機網頁易截斷網址讓人誤解是連線至正常網站，若未經審慎檢視，便容易受騙上當。同時強調在無法確認 QR Code 是否為真之狀況下，不輕易掃描 QR Code，且若連線成功後，尚需輸入個人、憑證或財務等敏感資訊時，更應三思而後行，經多方確認後，方可執行。

3.資安技術研析_AndoryuBot 新型殭屍網路研析

本季探討之資安技術研析為 AndoryuBot 新型殭屍網路研析，資安業者 Fortinet 於公開情資揭露 AndoryuBot 出現新型變種，以新型漏洞 CVE-2023-25717 進行感染擴散。此新型變種攻擊鎖定多個 Ruckus 無線產品為攻擊目標，無線產品若遭入侵成功後則可能被感染後成為 AndoryuBot 殭屍網路成員，並藉以發動分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)。

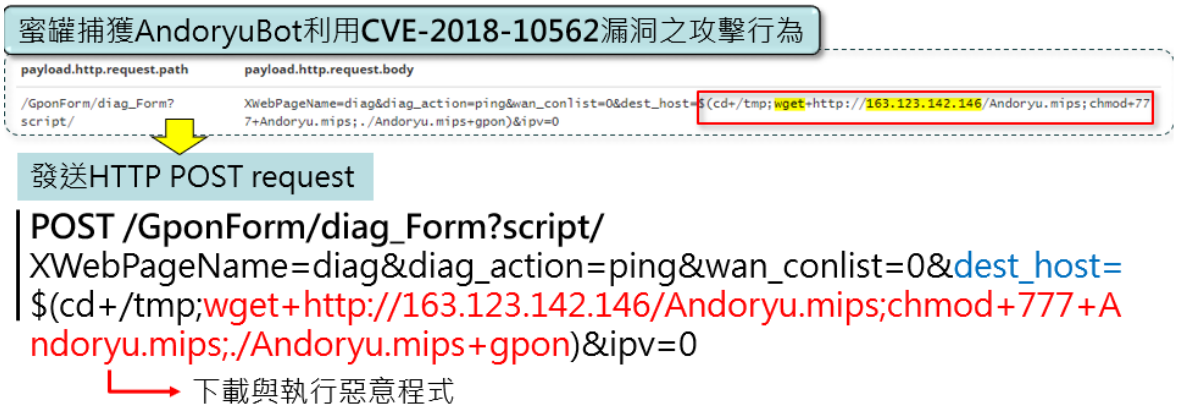
Ruckus Wireless 為國際知名之無線系統供應商，在此次所揭露之產品漏洞為 Ruckus Wireless Admin 介面存在跨站請求偽造(Cross-site request forgery, CSRF)與任意程式碼執行(Remote Code Execution, RCE)漏洞，藉以發送惡意請求，達到控制或破壞網路無線設備。研究亦發現駭客除持續利用該漏洞擴散殭屍網路，且發起各種協定之 DDoS 攻擊外，同時從社群媒體販售訊息亦發現，AndoryuBot 之駭客集團公開行銷 DDoS 攻擊服務，所提供之行銷方案包含每週或每月之各種攻擊次數套裝組合。

Ruckus 無線網通設備，雖銷售市場以歐美為主，但在亞洲亦有其客戶群。國家資通安全研究院掌握國際情資，利用蜜罐系統捕獲 AndoryuBot 殭屍網路活動，藉以觀測與分析此族群在台灣之網路活動與攻擊方式。以下將概述此殭屍網路於蜜罐誘捕情形，說明攻擊流程及提供防護建議。

3.1 漏洞說明與蜜罐誘捕

從蜜罐系統分析發現駭客族群攻擊與擴散對象包含多個物聯網設備與其他軟體漏洞，且從所捕獲 AndoryuBot 樣本之檔名，即可見以其族群名稱命名之特徵。駭客族群利用數項漏洞，經分析有 CVE-2023-25717、CVE-2018-10562 及 CVE-2016-20016 等以注入惡意指令攻擊，首先，以 CVE-2023-25717 RCE 漏洞為例，目標對象為 Ruckus 無線路由器，影響版本為 Wireless Admin Panels 10.4 以下之版本，此 AndoryuBot 新型變種透過

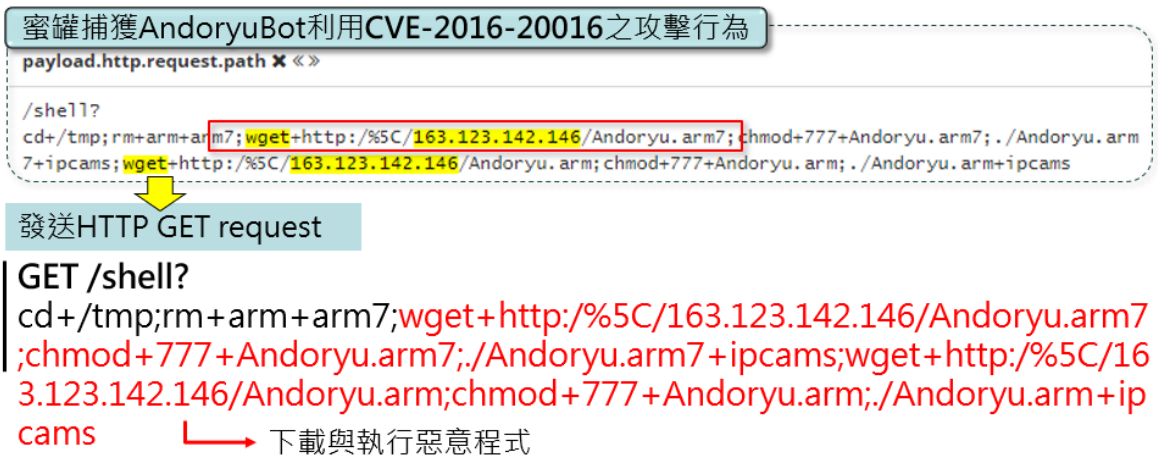
Ruckus 管理頁面之 URI「/forms/doLogin」繞過身分驗證執行指令注入惡意腳本下載安裝惡意程式，以達成感染目的；另一項遭利用之弱點為 CVE-2018-10562 RCE 漏洞，主要鎖定 GPON 路由器之 Web 管理介面之 URI「/GponForm/diag_Form」弱點，由於未對使用者送出之請求進行驗證與檢查，攻擊者可透過「dest_host」參數對 GPON 路由器進行命令注入攻擊，遠端操控設備，詳見圖 6。



資料來源：本報告整理

圖6　CVE-2018-10562 攻擊行為

最後捕獲之惡意樣本為利用 CVE-2016-20016 RCE 漏洞之攻擊行為，鎖定設備之 tv-7104he 與 tv7108he 韌體版本，相關設備之網頁管理頁面因 Shell 函數未對帶入之參數進行檢查，使攻擊者可進行遠端程式碼執行攻擊，詳見圖 7。



資料來源：本報告整理

圖7　CVE-2016-20016 攻擊行為

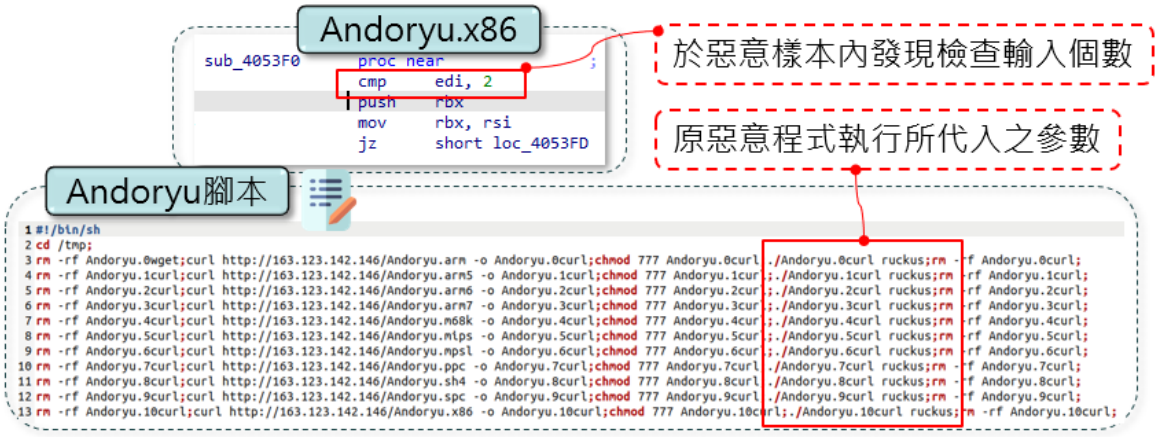
統計 AndoryuBot 殭屍網路針對上述漏洞之攻擊趨勢，上半年所偵測到攻擊連線，4 月為攻擊量最高峰，攻擊目標則多為越南。而分析蜜罐捕獲 AndoryuBot 下載腳本之漏洞攻擊，最常被利用之弱點為 CVE-2018-10562。從各國蜜罐誘捕資料得知，蜜罐 IP 受攻擊比例約為 0.5%，統計攻擊跳板來源 IP 數，共 3 筆利用 AndoryuBot 殭屍網路進行攻擊，皆為境外 IP，且因 IP 來自於一般電信業者之 ISP，故無法辨識發動攻擊之裝置類型。監測政府網際服務網(Government Service Network, GSN)網路資料，雖曾發現疑似以 CVE-2023-25717 漏洞嘗試攻擊 Ruckus 設備之行為，惟未發現裝置明確受駭之相關行為，故先針對相關 IP 發布警訊，提醒機關主動檢視防護措施，並後續將持續觀測 AndoryuBot 殭屍網路相關活動。

3.2 殭屍網路攻擊流程與修補建議

AndoryuBot 為本年開始活躍之殭屍網路，現從事件分析已知主要為啓動 DDoS 攻擊，干擾系統運作正常，而且從其發展趨勢得知此駭客族群建立此殭屍網路之目的與以往不同，預判未來可能朝向資安黑色產業鏈之趨勢發展，黑色產業鏈興起使駭客發展不同面向之攻擊模式，如鑽營漏洞攻擊、勒索軟體及憑證洩漏等，以獲取成功攻擊後之利得。以下將說明

AndoryuBot 殭屍網路攻擊流程，提醒機關隨時關注異常之軌跡。

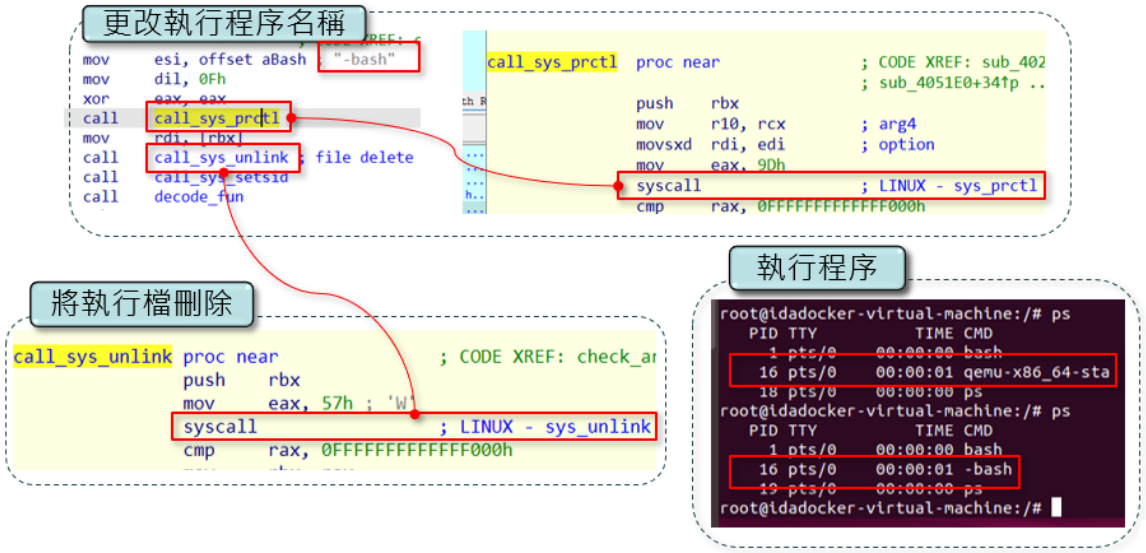
首先，當存在漏洞之 IoT 設備暴露於公開網路服務時，就能輕易被鎖定並注入惡意指令，執行惡意程式時皆以裝置名稱做為代入參數。駭客針對 Ruckus 路由器裝置注入惡意指令，執行指令設定為：./Andoryu.x86 ruckus。惡意程式執行時會先檢查參數數量，若輸入少於 2 個參數，則會直接結束程式，不執行任何動作，推測駭客直接結束程式之目的，可能為迴避沙箱分析與自動化分析機制，以及供駭客辨認裝置之用途，詳見圖 8。



資料來源：本報告整理

圖8　惡意程式檢查參數

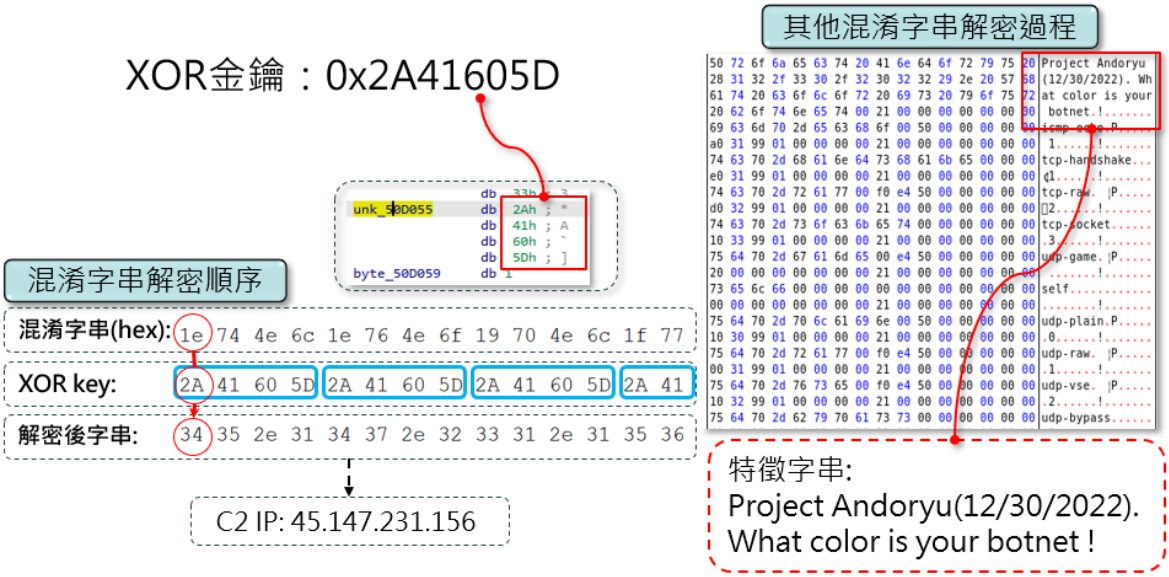
惡意程式執行後，AndoryuBot 透過 Prctl API 將自身執行程序名稱修改為「-bash」，以偽裝成正常執行程序，接續為清除軌跡，會使用 Unlink API 刪除本身程式，詳見圖 9。



資料來源：本報告整理

圖9　變更執行程序且刪除軌跡

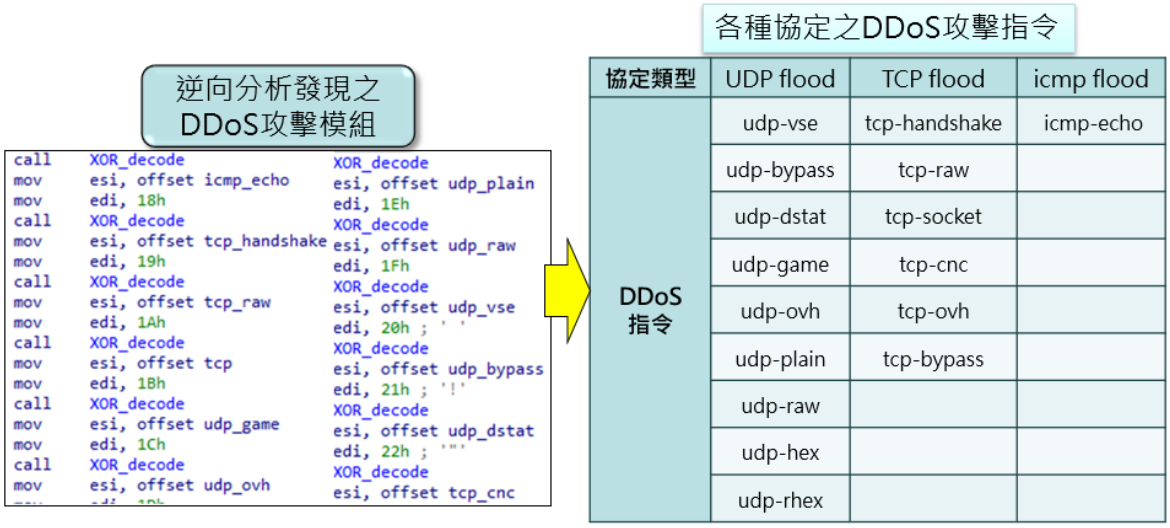
接續分析惡意程式內可發現駭客使用大量混淆字串，以規避靜態掃描惡意特徵，而透過分析取得 XOR 金鑰，解密混淆字串可取得 C2 IP 與多種 DDoS 模組，詳見圖 10。



資料來源：本報告整理

圖10 使用加密金鑰以規避靜態掃描

受駭裝置遭感染後，會發送 GET 請求向 IP 查詢網站之 API 取得受駭裝置 IP，再將 IP 回傳至 C2 伺服器並等待指令，以確保受駭裝置可正常連線與長期掌控。經逆向工程分析後，亦可見受駭裝置於等待 C2 伺服器發送指令後即可發動 DDoS 攻擊，並依據指令類型執行不同協定之 DDoS 攻擊，詳見圖 11。



資料來源：本報告整理

圖11 執行不同協定之 DDoS 攻擊

因應 AndoryuBot 新型變種攻擊方式，鑒於該漏洞利用入門檻低，且其概念性驗證(Proof of Concept, POC)已揭露於公眾，若有使用該產品者，應儘速更新修補程式，以降低遭已知漏洞入侵風險。由於此次是針對 Ruckus AP 設備之遠端管理介面之組態，所突顯之管理議題為不需開啓之遠端管理是否預設為關閉，且應定期檢視組態管理設定之適切性。另外，對於遠端管理連線之服務，則避免暴露至公開網路，以減緩可能遭攻擊之攻擊面。

未雨綢繆之作法應在挑選網路或系統產品前，訂定評選準則，挑選具備一定安全等級驗證之產品，並關注資安情資分享，檢視系統更新狀況。為避

免因漏洞入侵致提權之風險，基本上應訂定強密碼策略，輔以定期更新之要求，進階強化系統存取權限之管理，將使用者與系統皆設定為最小權限，或加入多因子與設備安全等驗證，且輔以網路異常行為之偵測與監控分析，以強化網路服務整體安全性。

4. 結論

本季具指標性案例駭客暗網與社群平台 AI 網路犯罪惡意程式，因相關惡意程式功能強大，讓購買者可以輕易使用工具展開網路釣魚攻擊活動，且提供 API 程式，協助簡化攻擊，預料將使這類攻擊案例大幅上升。另一起案例為知名駭客族群，使用外洩之憑證入侵成功，接續使用最新功能完善之變種惡意程式加密工具，加密遭鎖定之雲端儲存體。

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「AI 網路犯罪工具之資安管理」與「數位監視系統之資安管理」提出資安防護建議。

資安專題分享主題為 QR Code 網路釣魚攻擊，隨著 QR Code 因運用於各樣資通服務上之快速成長，衍生出大量 QR Code 網路釣魚攻擊，Quishing，為近年風行之網路釣魚類型。因 QR Code 本身為圖像檔案，防護機制可能無法偵測圖像檔案之連結是否為惡意，使這類型釣魚詐騙成功案例大幅篡升。且又因 Quishing 利用人員慣於使用個人行動裝置掃描 QR Code，當連線至駭客架設之外部伺服器後，內部網路安全控管與追蹤機制即無法辨識與追蹤，教育使用者不任意掃描 QR Code 仍為最佳解決方式。

另外，資安技術研析主題為 AndoryuBot 新型殭屍網路研析，此新型變種，以漏洞 CVE-2023-25717 進行感染擴散。鎖定多個 Ruckus 無線產品為攻擊目標，無線產品遭入侵成功後則可能被感染後成為 AndoryuBot 殭屍網路成員，藉以發動 DDoS 攻擊。機關應定期且全面檢視所擁有之資訊設備，關注系統更新狀況，警覺異常軌跡。