萬物聯網的資安威脅—談物聯網資安防護之道

吳啟文*、羅翊萍**

壹、前言

物聯網的應用廣泛，不管是在辦公環境、金融交易、交通運輸或醫療保健等，都已進入百家爭鳴的時代。物聯網的興起，帶給人類許多便利，並縮短彼此的距離，而以往封閉的系統與環境為追求連網的便利或發展應用服務之商機，也紛紛加入物聯網的懷抱，因此萬物聯網之發展已成為必然之趨勢。

然而，在物聯網快速的發展與設備安全性不足的情況下，提供惡意人士多元的入侵管道，同時由於物聯網設備無所不在且已實際運用於日常生活中，一旦被入侵所造成的影響規模將相當龐大，更嚴重可能還會影響民眾之基本生活。有鑒於此，本文藉由探討 5 起近年來所發生之物聯網資安案例，分析駭客運用之攻擊手法，歸納出物聯網常見之資安威脅，並提供資安防護建議與重點整理。此外，也將從資通安全管理法之角度，提供組織企業對物聯網資安防護與管理之相關建議。

*行政院國家資通安全會報技術服務中心主任。
**行政院國家資通安全會報技術服務中心科長。

貳、物聯網資安威脅與風險

依據國際研究顧問機構 Gartner 預測，108 年使用的物聯網終端裝置達 48 億個，比 107 年成長約 21.5%，到 109 年更將成長至 58 億個，成長幅度約有 21%。其中，公共服務將會是 108 年使用最多物聯網終端裝置的領域，包含住宅與商用之智慧電表等，其他如建築物自動化、車用及醫療照護等領域，在 109 年也有 25%以上的成長幅度。

然而，由於物聯網裝置數量過多又缺乏資安控制措施，因而成為駭客首選的入侵途徑之一，脆弱但規模龐大的物聯網裝置不僅能發動分散式阻斷服務（Distributed Denial of Service, DDoS）攻擊，還能進行挖礦、發送垃圾郵件或成為駭客入侵的跳板。趨勢科技零時差計畫（Zero Day Initiative, ZDI）統計 107 年上半年工業控制系統之監控與資料擷取（Supervisory Control and Data Acquisition, SCADA）系統相關漏洞數量，結果顯示 107 年之漏洞數量較 106 年下半年增加約 30%，與 106 年同期漏洞相較則接近 2 倍之多。此外，依據卡巴斯基所公布的 107 年上半年度報告，從物聯網裝置內發現的惡意軟體共有 121,588 種，比起 106 年的 32,614 種多出有 3 倍之多，駭客紛紛投入開發物聯網相關惡意軟體，欲從中謀取利益或建立入侵管道之攻擊手法，在現實社會層出不窮。

以下利用近期所發生的一些實際案例，來說明駭客是如何利用這些具有資安漏洞或缺乏資安控制措施的物聯網裝置，成功進行攻擊。

一、少爺殭屍網路

行政院國家資通安全會報技術服務中心（以下簡稱技服中心）發現駭客利用「少爺殭屍網路」，針對家用路由器進行攻擊，並誘騙利用該路由器連網之使用者下載惡意應用程式（APP），以達竊取個人資料之目的。截至 107 年 4 月，已有 20 多萬台路由器被駭客掌控，至少 6,000 台行動裝置遭感染，該 APP 不僅能取得手機型號、作業版本、系統及應用程式列表等資訊，還能竊取受害者的 APP 帳號、聯絡人資料及簡訊內容，並可遠端撥號、接收及寄送簡訊，洩漏的個人資料超過 100 萬筆，感染範圍擴及全球 55 個國家，少爺殭屍網路運作架構與感染流程詳見圖 1。

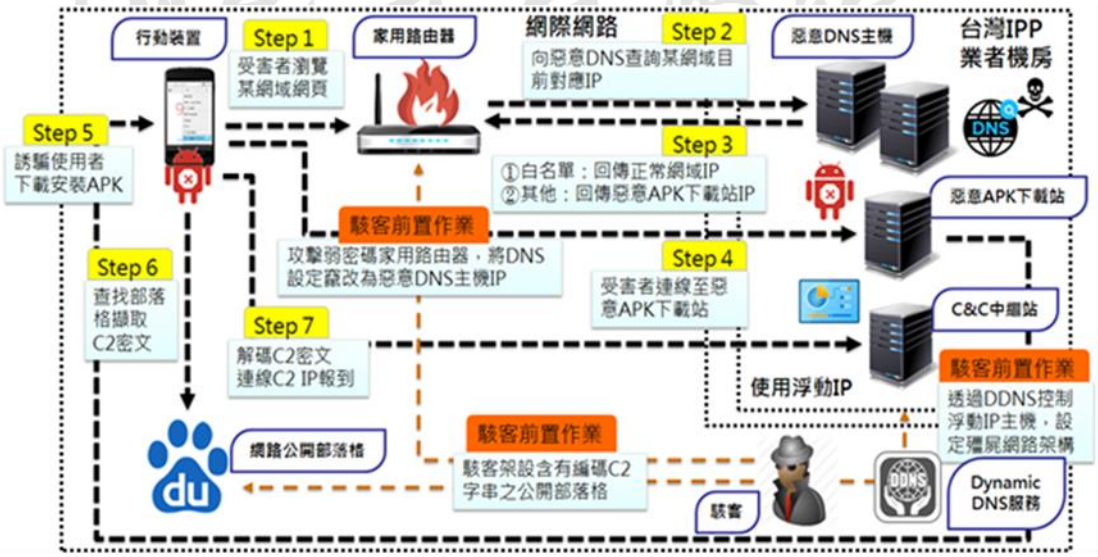


圖 1　少爺殭屍網路運作架構與感染流程

資料來源：本報告整理。

駭客藉由國外的雲端主機中介商，向臺灣網路平台服務商（Internet Platform Provider, IPP）租用 3 台浮動 IP 的雲端伺服器，建置一系列殭屍網路架構，其中包含惡意網域名稱系統（Domain Name System, DNS）伺服器、惡意安卓應用程式套件（Android application PacKage, APK）下載站台及做為命令與控制系統（Command and Control, C&C）伺服器。同時駭客利用浮動 IP 不斷變動特性，使得 IP 難以追蹤。除架設位於臺灣 IPP 業者的殭屍網路架構，駭客預先建立公開部落格用來存放 C&C 報到資訊，接著駭客須尋找弱密碼之路由器進行攻擊並修改其 DNS 設定，將 DNS 的 IP 更改為駭客自行架設的惡意 DNS 伺服器，如此方能達成少爺殭屍網路攻擊流程的前置作業。一旦安卓（Android）行動裝置透過被竄改 DNS 設定的路由器連線上網，將會被導向至惡意 APK 下載站 IP，並出現以正體中文、簡體中文、日文、韓文及英文 5 種語言製作的詐騙網頁，跳出「請安裝 Facebook 擴展工具包提升安全性，以及使用流暢度」的視窗（詳見圖 2），以假冒 Facebook 更新檔的方式誘騙民眾下載並安裝，達成感染裝置目的。

圖 2　假冒 Facebook 更新檔中文視窗畫面
資料來源：本報告整理。

二、環控系統入侵案例

技服中心透過殭屍網路威脅情蒐分析，發現位於某學術單位的環境控制（工業控制）系統，有來自不同國家之可疑 IP 的連線紀錄，詳見圖 3。為釐清是否有環控式殭屍網路，因此偕同教育部人員前往調查，進行封包側錄。

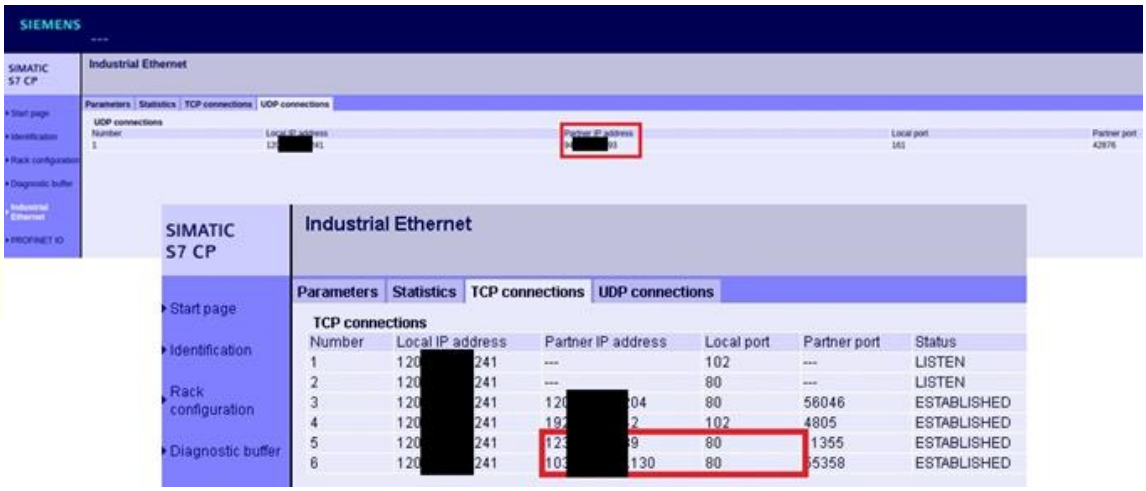


圖 3　環境控制系統 IP 連線紀錄
資料來源：本報告整理。

本次側錄的環境控制系統下串接電力、消防及污水等環境控制設備，該設備用以整合後端，並將資料傳回至人機介面（Human Machine Interface, HMI）環控管理主機，其目標主機網路架構詳見圖 4。

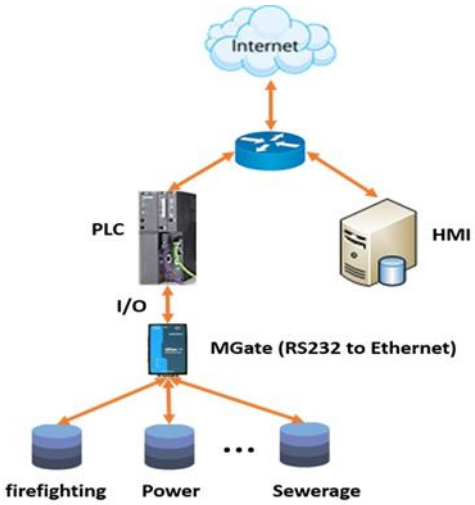


圖 4　目標主機設備網路架構圖
資料來源：本報告整理。

分析封包過程中發現，封包內容包含疑似物聯網惡意程式「Mirai」相關變種特徵，Mirai 殭屍網路持續攻擊此環境控制設備並嘗試散布惡意程式，主要透過 TCP 23（Telnet）連接埠對外擴散，利用 Telnet 連線與輸入常見的帳號密碼，嘗試感染其他物聯網設備，以加入「Mirai」殭屍網路。另外，部分殭屍網路會使用 PHP 的遠端程式碼執行（Remote Code Execution, RCE）弱點對外散布惡意程式。

經封包分析殭屍電腦資訊之統計，將事件之 IP 進行查詢 Banner，可辨識為何種類型的受害物聯網設備，其中數位視訊錄影機（Digital Video Recorder, DVR）監控系統為最大宗，可辨認的國內受害 DVR 設備數量為 230 台，國外受害 DVR 設備數量為 537 台，其餘未能辨識為何種類型的受害設備共有 2,424 個。相關情資透過國家資安資訊分享與分析中心

（National Information Sharing and Analysis Center, N-ISAC）進行情資分享，共發布 13 則 Bot 警訊給國家通訊傳播委員會，1 則 Bot 警訊給該受害機關。本次調查雖然並未發現駭客已入侵環境控制系統之明確跡證，但仍有部分收穫，其中掌握疑似 Mirai 變種特徵，得知 3 種惡意程式擴散途徑，並從分析過程中發現的下載站蒐集 12 隻物聯網惡意程式，調查中亦找到不少殭屍網路受害者並進行通報，將持續關注這類事件。

三、門禁系統入侵案例

Apache Struts 2 是一個開放原始碼的 Java EE 網站應用程式的 Web 應用框架。駭客利用 Struts 2 漏洞，植入惡意程式內容，以入侵門禁系統進行虛擬貨幣挖礦。

Apache Struts 官方於 106 年 3 月 6 日發布編號 S2-045 的資安漏洞，技服中心隨即於 106 年 3 月 7 日發布資安訊息警訊要求各機關儘速更新，後續該漏洞列入常見弱點與漏洞（Common Vulnerabilities and Exposures, CVE）之編號為 CVE-2017-5638。CVE-2017-5638 漏洞為駭客於 HTTP 協定表頭 Content Type 欄位，寫入由 Object Graph Navigation Language（OGNL）程式語言撰寫的惡意程式，Struts 2 解析 Content Type 內容認為需要進行檔案上傳，因此利用 Jakarta Multipart Parser 上傳套件執行該內容，駭客透過未檢驗與過濾解析內容之漏洞達到遠端執行程式

碼行為，HTTP Content Type 遭寫入程式碼示意圖，詳見圖 5。

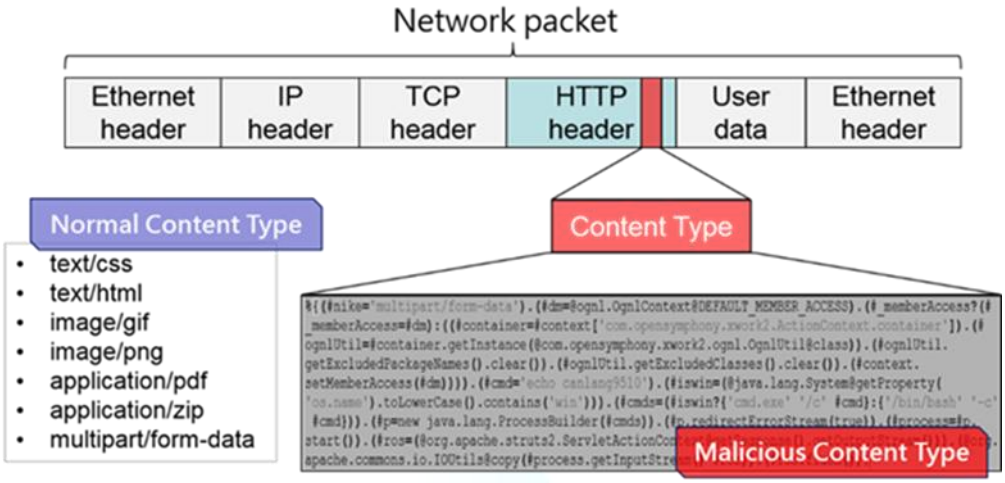


圖 5　HTTP Content Type 遭寫入程式碼示意圖

資料來源：本報告整理。

圖 5 顯示，網路封包於 HTTP 表頭 Content Type 欄位正常情況下，表示封包承載的資料類型，方便應用程式讀取封包時能利用對應方法進行解析。駭客利用 Struts 2 Jakarta Multipart Parser 上傳套件，其解析 Content Type 內容過程，會造成執行植入的惡意程式內容。漏洞揭露初期已經有概念驗證測試程式碼釋出，分析政府網際服務網（Government Service Network, GSN）HTTP 封包發現大量惡意 Content Type 內容及其變形，共觀察到 7,579 種惡意 Content Type 內容，萃取惡意 Content Type 內容進行手法分析，行為主要可分為漏洞測試、蒐集資訊、服務操作、使用者調整、權限調整、目錄操作、下載安裝、程序操作、檔案操作、執行程式、製作腳本及執行腳本等 12 種類別。以下進一步說明駭客如何

利用 Struts 2 漏洞入侵門禁系統進行虛擬貨幣挖礦之攻擊手法。

駭客利用 Struts 2 漏洞嘗試入侵目標系統，利用系統資源挖礦虛擬貨幣，分析入侵流程主要分為 4 個步驟，入侵流程圖詳見圖 6。

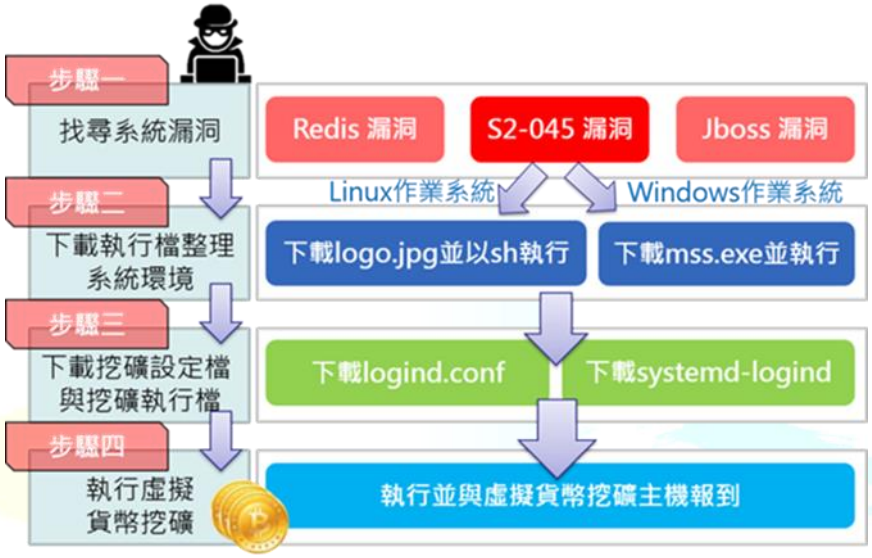


圖 6　利用 Struts 2 漏洞進行虛擬貨幣挖礦之流程
資料來源：本報告整理。

【步驟一】找尋系統漏洞：嘗試對目標系統進行漏洞探測，找出入侵切入點，依據外部情資顯示駭客也曾探測 Redis 與 Jboss 系統漏洞。

【步驟二】下載執行檔並整理系統環境：駭客依據作業系統而下載不同的執行檔，Linux 作業系統下載 logo.jpg，該檔案實際為 shell script 腳本檔，內容首先查詢虛擬貨幣挖礦相關執行程序並刪除，推測這行為可能要排除其他駭客挖礦執行程序，占據全部系統資源進行後續挖礦活動，接續從外部下載挖礦設定檔與執行檔。

【步驟三】下載挖礦設定檔與挖礦執行檔：設定檔內容為向虛擬貨幣挖礦主機報到所需要的相關資訊，並透過執行檔執行相關挖礦行為。

【步驟四】執行虛擬貨幣挖礦：駭客透過步驟三下載的執行檔讓受害系統進行挖礦。

同時，技服中心也進行內部分析並彙整 Struts 2 漏洞之相關情資分享予政府機關，包含下列 3 項惡意下載行為：

- 從 Github 下載後門或腳本程式：遠端攻擊者透過 Struts 2 漏洞對受害網站主機下達系統指令，從 Github 下載後門或腳本程式後在系統上建立後門或執行自動化腳本程式。
- 從外部網頁伺服器下載：遠端攻擊者透過 Struts 2 漏洞對受害網站主機下達系統指令，從外部網頁伺服器下載惡意程式，並觀察到前 10 大下載次數的外部網頁伺服器威脅 IP。
- 從檔案傳輸協定（File Transfer Protocol, FTP）伺服器下載腳本程式：遠端攻擊者透過 Struts 2 漏洞對受害網站主機下達系統指令，透過 FTP 協定下載腳本程式並執行，觀察受害網站主機連線至外部威脅 IP，已將該 IP 列於黑名單中，並觀察近期仍有惡意檔案下載行為。

四、Android Root Bridge 漏洞利用

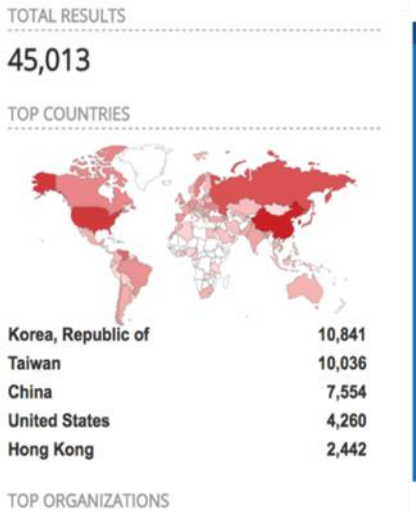
技服中心發現安卓（Android）系統建置的公車站電子看板，存在 Root Bridge 漏洞，此漏洞的存在，易遭駭客入侵散布惡意程式，並發動 DDoS 攻擊，進而被植入挖礦程式，以賺取虛擬貨幣。經研究分析發現，除北韓駭客利用這個漏洞，植入挖礦程式以獲取利益外，亦有中國網路犯罪集團利用相同漏洞，植入殭屍程式控制智慧裝置，並針對特定購物網站發動 DDoS 攻擊，讓購物網站無法正常提供服務，藉以對商家進行金錢勒索。

由於公車站電子看板為交通領域關鍵基礎設施的一環，萬一遭駭客入侵控制，可能造成交通控制系統停擺，引起交通錯亂，進而危害市民生活或是造成更嚴重的後果。駭客甚至可利用電子看板公告不實的資訊引起民眾恐慌，如駭客透過電子看板散布假新聞與公告等，將對臺灣政治或民眾生活造成不可抹滅的危害。

在分析 Root Bridge 漏洞之前，必須先介紹 Android Debug Bridge（ADB）。ADB 是用於安卓開發使用的指令工具，可以直接控制安卓模擬器或真實的安卓裝置，進行除錯、測試、上傳及下載等工作，一般開發多使用實體 USB 進行連結，但也可以開啟網路連線管理功能（預設連結埠為 5555），透過網路同時連結多個裝置進行除錯。

這個管理介面通常是開發商用來進行系統管理與應用程式開發使用，在非開發者版本應該被停用。惟部分連網裝置卻因管理失當或錯誤使用 ADB 功能，導致受害裝置能透過 5555 連結埠進行連線，使任何人在不需認證的情況下，即可獲得系統最大權限（Root Shell）操作該連網裝置。一旦駭客利用 Root Bridge 漏洞入侵受害裝置後，即可在受害裝置上安裝惡意 APK，使得受害裝置除進行挖礦作業外，還會掃描網路上的其他 ADB 裝置（連結埠 5555），企圖擴散感染。

此次遭攻擊的安卓智慧連網裝置，甚至包含智慧城市與智慧校園中用來公告訊息的多媒體電子看板。進一步以網路引擎進行搜尋與統計顯示，遭受漏洞攻擊的裝置遍布全球，總計超過 45,000 台安卓裝置存在管理漏洞，臺灣存在弱點的裝置數量位居全球第二（詳見圖 7），這些智慧裝置產品包含一般民眾經常使用的智慧電視、電視盒、安卓手機及平板等，共計 1 萬餘台。遭受駭客入侵的安卓智慧連網裝置會被竊用運算資源，進行挖礦與殭屍網路擴散等非法行為，除占據網路頻寬影響網路使用效能外，還會被盜取裝置內使用者資料，造成民眾個人隱私外洩。



Device Name	Model Name	Device Type	Count
Samsung Galaxy Note 3	SAMSUNG-SM-N900A	Android Smart Phone	2904
Motorola Moto X (Europe)	XT1052	Android Smart Phone	2886
Google Pixel XL	Pixel XL	Android Smart Phone	472
Google PIXEL 2 XL	PIXEL 2 XL	Android Smart Phone	454
Samsung Galaxy S5	SM-G900F	Android Smart Phone	436
OnePlus 3T	ONEPLUS A3010	Android Smart Phone	360
OnePlus 5	ONEPLUS A5000	Android Smart Phone	358
Samsung Galaxy S8 Plus	SM-G955F	Android Smart Phone	337
Samsung Galaxy S8	SM-G950F	Android Smart Phone	335
Samsung Galaxy S4	GT-I9500	Android Smart Phone	100
EVPAD PRO 電視卡盒	EVPAD-PRO-T	Android TV box	56
EVPAD PRO 電視卡盒 台灣版	EVPAD-TW-MAX	Android TV box	46
Asus ZenFone 5	ASUS T00J	Android Smart Phone	44
MXQ PRO 4K s905 p201	Android p201	Android TV box	43
EVPAD PRO 電視卡盒	EVPAD-PRO-MAX	Android TV box	33
Sunchip TV box	CX_A39	Android TV box	33
Unblock Global Edition S800	Global_Edition_S800	Android TV box	30
RockTek A2V	RT_A2V	Android TV box	24
Askey Set-top box	STI6030	Android TV box	24
JVC 65T	65T	Smart TV	21

圖 7　網路搜尋存在漏洞之連網裝置

資料來源：本報告整理。

分析並推測造成漏洞的最主要原因，在於使用者自行使用 Root 權限開啟 ADB 連線功能。一般民眾可能參考網路上的教學文章，自行使用坊間流傳的權限提升（俗稱 Root）工具並參照教學流程，對安卓系統的手機、平板、智慧電視及電視盒進行權限提升，以達到自行安裝非官方的 APP 或盜版程式的目的，但卻也因此造成許多智慧電視與電視盒在提高權限的過程中被開啟 Root Bridge 漏洞，導致智慧家電遭受入侵。

五、MikroTik 路由器弱點

MikroTik 是位於歐洲拉脫維亞的知名網路公司，其商品包含路由器與相關網通設備，目前全球已知的使用數量約 1,879,520 台，市占率為 2.8%。MikroTik 傳出遭駭客利用安全漏洞，透過 MikroTik 路由器的漏洞（CVE-2018-14847 與 CVE-2018-1156），攻擊者可入侵受害設備取得 Root

Shell 權限，並竊取受害設備相關資訊，該漏洞在常見漏洞評分系統（Common Vulnerability Scoring System, CVSS）分數為 7.5 分與 9 分，皆為高風險。主要產品 RouterOS 係基於 Linux 作業系統，可安裝於一般電腦使其變成路由器設備，且無需高規格的硬體要求，又因 RouterOS 擁有許多功能，包含防火牆（Firewall）與虛擬私人網路（Virtual Private Network, VPN）等，具備相當多的管理權限。

107 年 4 月 MikroTik 路由器被揭露 1 個目錄瀏覽的弱點，CVE 編號為 CVE-2018-14847，屬於中風險弱點。遠端攻擊者能通過修改請求來繞過身分驗證，並可讀取任意檔案。依據這個弱點延伸出其他弱點，其中較為嚴重的為 CVE-2018-1156 之身分驗證的 RCE 弱點，可允許攻擊者取得完整的系統存取權。隨著 107 年 10 月釋出一段新的概念驗證程式碼，又使風險程度提高，遠端攻擊者能在受漏洞影響的 MikroTik 路由器上執行遠端程式碼，攻擊手法詳見圖 8。

圖 8　駭客利用 MikroTik 路由器漏洞之攻擊手法

資料來源：本報告整理。

依據 108 年 1 月 14 日 Shodan 統計數，MikroTik 在全球的使用量共 1,879,520 台，排名前 5 之使用國家分別為巴西（250,129 台）、中國（190,830 台）、印尼（142,513 台）、俄羅斯（134,837 台）及伊朗（91,722 台），MikroTik 在臺灣的使用量則有 13,156 台，故全球所傳出之災情，受害者遍及全球。

六、小結

以往要實現 DDoS 攻擊並不容易，但隨著物聯網裝置的攀升，而大多數的物聯網裝置皆以能快速投入市場為目標，忽略其資安議題，使得相關資安事件層出不窮，這些資安事件也喚起大眾對物聯網資安議題的重視程度。綜整上述資安威脅案例，歸納出常見的物聯網資安風險如下：

- 物聯網設備或相關系統未納入盤點。
- 認證與存取權限相關設定有誤。
- 設備軟／韌體資安漏洞。
- 使用者或操作人員資安意識不足。

參、物聯網資安防護重點

物聯網已然成為現今資訊科技發展不可或缺之趨勢，資安事件的發生也預告風險發生的可能性逐步升高，依據 Gartner 預測，108 年在物聯網安全方面的支出達 19 億美元，包含端點安全、網通安全及專業服務等，到 110 年更將達到 31 億美元，足以顯示物聯網安全已成為全球所關注並計畫重點投資之議題之一。

以下因應物聯網資安威脅，逐一說明上述物聯網資安案例之相關管理及資安防護建議，並進一步綜整出物聯網之資安防護重點，提供使用者與相關資安人員參考。此外，針對所列之物聯網資安防護重點，以資通安全管理法（以下簡稱資安法）之角度說明其管理與防護重點，供組織企業參考。

一、資安防護重點

以下針對上述 5 起資安威脅案例，分別說明其相關資安防護建議：

（一）少爺殭屍網路

少爺殭屍網路主要攻擊弱密碼的家用路由器，並竄改 DNS 為惡意之 DNS 主機 IP，以誘騙使用者下載並安裝假冒的更新檔，達感染之目的。為避免感染少爺殭屍網路，提出以下 5 點防護建議：

1.路由器應避免將管理介面外露在公開網路。

2.更改設備出廠時預設的帳號密碼，且不要使用過於簡單的密碼。

3.定期更新廠商推出之最新版本韌體，以減少遭受已知漏洞的攻擊機會。

4.檢查路由器相關設定是否遭竄改。

5.在使用行動裝置瀏覽網頁時應提高警覺，當出現異於平常的網頁或通知訊息，切勿點擊不明連結或安裝未知來源的 APP，以免裝置遭受網路攻擊之風險。

（二）環控系統入侵案例

環控系統入侵案例為疑似物聯網惡意程式 Mirai 之相關變種，主要透過 TCP 23（Telnet）連接埠對外擴散，利用 Telnet 連線與輸入常見的帳號密碼，嘗試感染其他物聯網設備，以加入 Mirai 殭屍網路。為避免感染 Mirai 殭屍網路，應更改設備出廠時預設的帳號

密碼，且不要使用過於簡單的密碼。

（三）門禁系統入侵案例

該漏洞主要是 Apache Struts 2 負責處理檔案上傳封包的 Jakarta Multipart Parser 解析程式存在弱點，讓遠端攻擊者可寄送含有惡意 Content Type 封包，造成攻擊者可遠端執行任意程式碼，進而植入惡意程式內容，達入侵門禁系統進行虛擬貨幣挖礦之目的。為避免駭客利用 Strust 2 漏洞，使用者應確認網站主機是否使用 Apache Struts 2 的網頁應用框架，可透過檢查網站主機目錄中「WEB-INF\lib\」資料夾內的 Struts2.jar 檔，確認當前使用的版本。如所使用的 Apache Struts 2 為受 CVE-2017-5638 漏洞影響之版本，則須更新官方 Github 所釋出最新之 Apache Struts 版本。

（四）Android Root Bridge 漏洞利用

駭客利用 Root Bridge 漏洞入侵安卓受害裝置，即可在受害裝置上安裝惡意 APK，使得受害裝置除進行挖礦作業外，還會掃描網路上其他 ADB 裝置(連結埠 5555)，企圖擴散感染。為預防 Root Bridge 漏洞所帶來的資安威脅，提出以下 5 點防護建議：

1. 勿隨意對裝置進行權限提升動作，以避免開啟不必要功能。

2. 若無使用上的需求，應關閉裝置的遠端管理功能，減少裝置被攻

擊的途徑。

3. 勿隨意在裝置上安裝來路不明之應用程式，並留意應用程式所要求之存取權限。

4. 若需使用遠端管理功能，應避免將裝置管理介面曝露於網際網路，並完備權限存取控制。

5. 若裝置有被植入惡意程式的疑慮，可使用回復出廠設定的方式，以清除惡意程式。

（五）MikroTik 路由器弱點

MikroTik 路由器弱點之起因為 1 個目錄瀏覽弱點，駭客可利用該弱點取得管理員登入憑證並進行解密，再搭配存在之開發者後門機制，從遠端取得 Root Shell 訪問許可權。為避免駭客透過此漏洞攻陷 MikroTik 路由器，MikroTik 使用者應確保已修補 CVE-2018-14847 路由器漏洞。

觀察上述物聯網資安威脅案例之相關防護建議發現，物聯網的資安風險不僅發生於該物聯網設備，也可能發生於與設備相連之相關資通系統，因此即便一個小環節的失誤，都將造成資安事件進而影響設備或人員，甚至影響交通、電力、消防及污水等關鍵基礎設施。

綜整上述對於各威脅案例之防護建議，以下提供物聯網資安防護重點，期能從小環節來強化物聯網資通安全：

- 避免採購具資安疑慮之物聯網資通設備：針對資料外洩事件或資安漏洞頻傳之物聯網資通設備，應以白名單或黑名單方式管制相關採購。
- 盤點物聯網資通設備：物聯網設備眾多，應定期盤點相關設備並視需要更新。
- 修改預設密碼：物聯網設備通常具備連網功能，於正式上線前，刪除預設帳號或更新密碼是基本防範之道。
- 建立存取控制機制：限制物聯網設備相關應用程式與元件之權限，只提供該設備之必須或最小權限。
- 進行安全更新或程式升級：相關物聯網設備應如同其他資通系統定期執行安全性更新，並時時關注漏洞之發現，提供防範機制。
- 關閉不必要的通訊服務：關閉物聯網設備相關通訊服務，只提供該設備之必要或最少服務功能。
- 定期檢測物聯網設備：發展或採用第 3 方認證之物聯網資通設備檢測機制，智慧電視、路由器、網路攝影機、網路印表機及門禁系統等辦公室連網設備，也都應考量包含在檢測範圍內。

- 提升物聯網資安意識：勿隨便下載來路不明之檔案或應用程式，也勿點選可疑之連結，更勿任意修改非官方認定之系統參數與功能。

二、資安法角度之物聯網資安防護重點

資安為達成萬物聯網成功之基石，有鑒於資安事件層出不窮，為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，資安法於 108 年 1 月 1 日起正式施行，除象徵政府積極在各個層面架構國家層級資安防護設施外，亦成為我國資安發展眾所矚目的里程碑，更是重要的法規基礎。

資安法將關鍵基礎設施納入重點保護範圍，包含能源、水資源、通訊傳播、交通、金融、高科技園區及緊急醫療等領域，而在關鍵基礎設施中物聯網扮演著關鍵的角色，即便再小的連網裝置，一旦被入侵都足以癱瘓與民生相關之系統，進而動搖國本。資安法的制定再再顯示對於物聯網安全的重視，期透過法律強制之要求，達到重要資通訊環境之安全完備度。

資安法的重點主軸包含以下 2 點：

- 訂定、修訂及實施資通安全維護計畫，並定期以稽核等方式檢視該計畫之完備程度，若有缺失或待改善者，則應提出改善報告，並持續改善。

- 訂定資通安全事件通報及應變機制，並完備其通報及應變程序。

在面對一個新法的通過時，組織勢必要規劃相當的資源投入，以因應接踵而來的挑戰。而針對上述資安法之重點，參考目前規劃之資通安全維護計畫應備項目與物聯網的資安防護重點，以下提供物聯網安全之資安管理與防護建議，以縮小適法性之差距。

- 盤點物聯網設備與資通系統，並進行資安風險評估：標示物聯網核心資通系統及相關資產，釐清核心業務及其重要性，以落實物聯網資通系統之安全管理，並依盤點結果範圍執行資安檢測與評估資通安全風險，瞭解如資訊儲存區域、組織面、實體面、技術面及作業面等資通安全風險，再依風險評估結果，訂定適切之資通安全防護及控制措施。

- 落實物聯網系統委外資安管理，訂定資通系統或服務委外辦理之管理措施：若有委外辦理資通系統之建置、維運或服務之提供，應選任適當之受託者，並適時進行監督與管理。

- 提升人員資安意識：規劃對物聯網裝置與設定之資安教育訓練並進行資安專業人才培訓機制，強化內部人員之物聯網資安核心能量。

- 訂定通報應變機制並落實通報應變程序：當發生物聯網裝置或物聯網系統相關之資安事件時，應遵循所制定之資通安全事件通報應變流程向相關上級、主管或監督機關進行通報，並提出資通安全事件調查、

處理及改善報告。

肆、結論

伴隨萬物聯網的時代來臨，物聯網裝置或相關科技應用已隨處可見，而由於物聯網便利之連網特性被廣泛使用，也成為駭客首選的入侵路徑之一。本文藉由對「少爺殭屍網路」、「環控系統入侵案例」、「門禁系統入侵案例」、「Android Root Bridge 漏洞利用」及「MikroTik 路由器弱點」等 5 起物聯網事件之探討，瞭解駭客所攻擊的物聯網設備、管道及手法相當多元，攻擊管道主要藉由物聯網設備之弱密碼、資安漏洞及資安意識不足等進行攻擊，攻擊之手法包含誘騙使用者下載並安裝惡意 APK、植入惡意程式發動 DDoS 攻擊、植入挖礦程式獲取利益及取得管理員登入權限等入侵方式，而受害的物聯網設備更是五花八門，包含路由器、智慧電視、智慧家電、個人行動裝置及數位視訊錄影機，甚至到與電力、消防及污水連接之環境控制系統、辦公環境之門禁系統及公車站電子看板等基礎設施都成為受害目標。

在這萬物聯網的時代，任何存在於你我生活周遭之物聯網設備，都有可能成為下一個駭客攻擊的目標，因此本文亦提供物聯網的資安防護重點供民眾與資安人員參考，包含避免採購具資安疑慮之物聯網資通設備、盤點物聯網資通設備、修改預設密碼、建立存取控制機制、進行安全更新或程式升級、

關閉不必要的通訊服務、定期檢測物聯網設備及提升物聯網資安意識等。同時，也從資安法角度，提供組織企業在規劃發展物聯網安全時，應考量的資安管理與防護建議。最後，面對駭客詭譎多變的攻擊手法，有效落實相關防護措施才會是真正的物聯網資安防護之道。

參考文獻

EGHAM (2019), Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020. Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io

Kaspersky (2018), New IoT-malware grew three-fold in H1 2018. Retrieved from: https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018

STAMFORD, Conn. (2018), Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018. Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

TrendMicro (2018), 2018 Midyear Security Roundup. Retrieved from: https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf