當門禁系統成為駭客的挖礦機

■臺北市立中正高中資訊組長　李詩婷

物聯網的時代來臨，新興科技帶來便利的同時，背後也隱藏了重大的資安風險，機關在採購相關設備時也要小心謹慎，減少資安事件發生的機會。

門禁系統潛藏安全漏洞

好萊塢特務電影的駭客，只要手邊有一台電腦就能控制任何資訊系統，從屏蔽大樓監視器的畫面，或是遠端控制門禁鎖，讓人輕易地進出機關重地等都只是小菜一碟。以上場景觀眾已經司空見慣，但若以為這些只會出現在電影裡那就是大錯特錯了，隨著駭客手法日新月異，電影中的許多情節都已成真。

《台灣電腦網路危機處理暨協調中心(TWCERT／CC)》於去(2017)年9月時就發出警告，數個特定考勤門禁系統中已被發現存在資安漏洞，可能被駭客利用而植入木馬或後門等惡意程式，不僅具有機敏資訊（例如內部人員出勤紀錄、員工編號或帳號密碼等）外洩的風險，而且可能被駭客進一步取得系統完整的控制權。

「運算資源」成為駭客覬覦目標

不要以為駭客只會針對資料有興趣，就心存僥倖。許多資安事件案例顯示，駭客想竊取的已不只是有價值的「資料」，而是轉為鎖定裝置的「運算資源」。典型的攻擊手法是植入殭屍（bot）病毒，成為

受駭客控制的殭屍電腦，潛伏並隨時等候駭客下一步命令，一旦殭屍網路大軍成形，就能用來發動分散式阻斷服務攻擊（DistributedDenial-of-Serviceattack,DDoS），讓雲端服務或網站連線負載量過大而造成服務停擺。

除此之外，新型態的攻擊手法則是植入比特幣挖礦的惡意程式，讓裝置搖身一變成為駭客專屬的虛擬貨幣挖礦機，不僅難以追查，還能立即替駭客帶來金錢上的利益，比過去還要設法販賣機敏資料或向被害企業組織勒索贖金更方便省事。

物聯網裝置成為駭客眼中的肥羊

門禁卡感應、指紋辨識、車牌辨識等門禁系統皆屬於物聯網（InternetofThings,IoT）技術的應用，物聯網是近年來最火紅的技術之一，其應用例如智慧家電、居家安全偵測及監控系統或穿戴式裝置等，並可與監控系統、網路、中央控制等系統整合，以進行數據收集與遠端控制。

然而，在一窩蜂擁抱物聯網技術的熱潮中，不得不重視的是其背後所隱藏的隱私問題和資安風險。據資安業者卡巴斯基實驗室（KasperskyLab）調查，光是去年就出現逾四千種新 IoT 惡意程式，遠高於前年的 3,219 種。

分析 IoT 惡意程式如此蓬勃發展的原因，是因為物聯網裝置具有

以下特性，故容易成為駭客攻擊的目標：

一、資通安全易被忽略

人們通常會專注於保護個人電腦和智慧型手機的隱私，但卻容易忽略物聯網裝置的資安風險。在僥倖心理下，即使知道所使用的裝置系統已有安全漏洞，也可能因為成本預算及人力等考量而無法進行產品升級或汰換。

二、與一般電腦存在同樣的安全問題

隨著物聯網裝置功能需求提高，裝置內部所使用的作業系統也向一般使用者電腦貼近，以應付高階的運作需求。以物聯網裝置可能搭載的 Linux 嵌入式作業系統為例，其內部的核心（Kernel）與上層應用軟體和函式庫也可能存在與一般電腦相同的安全漏洞。例如 2014 年 9 月曾爆發的 ShellShock 重大漏洞（CVE-2014-6271），可能造成目標主機的機敏資料洩露或甚至被駭客所控制，影響的範圍主要為使用 bashshell 的作業系統，包含 CentOS、Ubuntu 及 MacOSX 等，而亦有不少 Linux 嵌入式作業系統內建了 bashshell，故同樣存在資安風險。

三、安全性漏洞修補頻率低

在電腦或是手機上還有多種防毒軟體可以安裝使用，例如微軟、Apple 或 Google 等亦常會釋出安全性修補程式，但卻少有針對物聯

網裝置開發專門的防護軟體，只能仰賴裝置製造商釋出的韌體（即燒錄於硬體內的軟體）更新。在成本的考量下可能無法於一年內更新一次，且即使製造商釋出了更新，使用者端也不具備自動修補的能力，故常見的狀況是裝置的韌體未更新，最後只能以汰換硬體收場。

四、常使用預設的帳號密碼

物聯網裝置為了方便進行大量生產，往往會使用預設的帳號密碼，這種現象可能出現於同一個型號的產品或甚至同一個產品線的所有裝置，且工廠出貨後部署至使用者端時，裝機人員也不會特定去修改裝置的預設帳號密碼，甚至可能無法修改，故大開駭客方便之門。駭客只要鎖定共同供應契約清單上所列的裝置，一旦成功破解，則採購同一型號的機關組織皆有被入侵的風險。

五、不易發覺異常

功能需求及成本考量下，物聯網裝置本身往往不需具備大型的使用者螢幕，僅需顯示必要訊息（例如通行碼或異常燈號），故入侵行為也不易被直接發覺。

六、長期不關機

駭客入侵成功後，除了要避免被資安設備察覺，還需要確保惡意連線的暢通，否則好不容易攻下的據點若隨時會失效，那就不符合攻擊的時間成本。而物聯網裝置的需求就是要能隨時提供服務，例如門

禁系統必須 24 小時開啟，且隨時連結網路，一旦被成功入侵就可讓駭客長時間使用，可能被當作駭客的跳板機或是殭屍網路成員，長期潛伏並靜待駭客下達攻擊命令。

結論

現今的物聯網資安防護仍相當脆弱，特別是在連網裝置端點上的安全防護更是被人所忽略，全球的物聯網裝置於 2020 年預估會成長到二百至五百億台，更顯出潛藏資安問題的急迫性。資安專家建議使用者在架設物聯網裝置時，應變更裝置的預設帳號密碼，且不要讓裝置暴露在公開網路上讓人隨意存取，並且關閉系統尚不必要的網路服務，以防有心人士惡意探測系統上的漏洞；若設備有疑似遭到入侵的跡象或異常行為，應立即聯繫相關設備廠商重新安裝系統或更新韌體版本。只要遵行這幾項建議，即可大幅降低資安風險，減少被惡意程式狙擊成功的機會。

（※本文摘錄自法務部調查局 107 年 1 月號清流雙月刊）