行動裝置的資安危機

◎林穎佑

隨著科技進步，智慧型手機及平板電腦已非常普及，正在改變民眾的生活習慣。現今隨著行動上網技術的進步，人們可以隨時隨地上網，但在方便之餘，也衍生許多資訊安全的問題。根據統計，2014 年 4 月惡意與高風險行動裝置已突破二百萬支。值得注意的是，行動裝置遭到入侵，其損失不會只有手機上的資料，透過「雞蛋全部放在同一個籃子」的雲端科技，將使資安問題更加擴大。

對現代人來說，智慧型手機已是許多人的生活必備品，經由智慧型手機可以與雲端連結，達到收發信件、資料儲存、線上交易（網路銀行、電子商務）等功能，無形中讓智慧型手機內部的資料成為駭客覬覦的目標；特別是在雲端管理上，雲端科技的應用主要是依賴行動數位傳遞，讓使用者的每一個端點都能連結到資料庫，並透過技術使其達到即時共享與傳遞資訊的功能；但這也代表只要有一端失守，就可能造成整個雲端防線的崩解，而在遭到入侵當下，雲端系統商又因必須保持與其他作業系統端連線而不能立即斷線維修。這讓有心人士開始嘗試攻擊防護相對薄弱的智慧型手機，並藉此作為日後侵入其他資料庫（如 FB 帳號、電子郵件信箱、線上交易平臺）的跳板，達到竊取個人帳戶資料密碼之目的，方便日後在黑市兜售，藉此獲取更大的利潤（如販賣信用卡資料、竊取帳戶、假身分申請手機或金融帳戶等）。

軟體的風險

目前一般民眾在下載手機應用軟體時，最容易忽略其帶來的風險。APP 軟體是 Application 簡稱，其特別指為手機所設計的應用軟體。依據目前主要的三種智慧手機平臺：蘋果的 IOS 系統、Google 的 Android，以及較少人使用的 Window 系統，許多軟體商都針對這些系統設計出搭配的應用軟體。一般人在下載 APP 軟體時，都只注意其便利性及實用性，卻忽略在授權給相關軟體開發商時，可能也在無意間「同意」授權軟體商取得許多使用者的資料，像是通訊錄、GPS 定位紀錄（藉此追蹤使用者位置），甚至是線上遊戲紀錄。因此在使用類似軟體時，或許已洩漏了許多重要資料給有心人士。如近年來風行兩岸的交友聊天程式，便傳出其通話紀錄會遭到第三方側錄並傳送到某國的消息。有鑑於該通訊系統在外國並不普及，因此該公司重新在新加坡設立新公司，並將交友軟體重新命名推出，期望藉此打入市場。雖然就系統商而言，是需要消費者適當地回饋使用意見，藉此來強化其系統功能以及改善缺點，但若是駭客藉此竊取個資加以應用，例

如進行網路詐騙、利用個資於通訊軟體之通訊錄發送惡意連結等，便是目前難以防範的弱點。除了部分廠商有系統地蒐集資料外，更有許多駭客直接仿造知名 APP 軟體，放置在網路空間提供使用者下載。對一般消費者而言，分辨是否由官方發布的 APP 軟體是有相當程度的困難；且在價格的考量下，若能以較低廉的價格取得相同的價值，通常能有效吸引消費者下載，特別是許多軟體都標榜著免費下載，更具有相當吸引力。

除了竊取資料之外，行動裝置惡意軟體也從一開始相對無害地彈出廣告訊息，希望使用者點擊以增加廣告收益；一路演化到今日的高費率服務盜用程式（主動幫被害人撥打高付費電話，或主動下載需要較高花費的其他軟體）、後門程式，甚至是 Rootkit 駭客工具，以及新出現的手機綁架軟體（透過 APP 系統控制對方手機，要求對方付出高額「贖金」才予解除控制）。此外透過 Onion Router 惡意程式（一般俗稱 TOR）更可讓使用者在網路上「匿名」；網路犯罪者會利用 TOR 來隱藏自己的行蹤，並連上伺服器來遠端遙控受害者的行動裝置；一旦成功建立連線，便可透過此方式執行一些惡意行為，如：撥打某些高額付費電話、攔截並讀取文字簡訊、將簡訊發送至特定號碼等。使用 TOR 可讓犯罪者的行蹤更難被追查，也更難追蹤其幕後操縱的伺服器。

硬體的選擇

而在硬體方面，先前在臺灣掀起搶購風潮的大陸製手機（小米機），也傳出其手機在設計上，已植入會定期回傳資料的相關程式，曾引發許多討論。目前廠商已坦承手機會將用戶個人資料回傳到小米北京伺服器，但強調小米將消費者資料回傳至北京，是為了對應消費者身分資料是否可以使用其他通訊功能。惟根據許多資訊安全公司的測試指出，小米機會傳送手機的 IMEI、IMSI 碼號、個人資料與簡訊。這對小米機的使用戶造成負面影響，擔心是否還有更多竊資行為只是尚未公布。畢竟從技術面上，透過鎖定特定手機用戶，利用遠端遙控方式，可以打開目標的麥克風，甚至攝影機鏡頭，藉此達到竊聽與偷窺的目的是可行的。而也有言論指出其他國家的品牌，也有類似的機制，因此只要是使用手機便有個資外洩可能。如之前發生的史諾登事件中，便有指出美國政府透過稜鏡計畫來達到監聽之目的，而許多網路、通訊公司也在其配合名單之中，這些新聞都一再顯現出智慧型手機的資安問題。

此外，智慧型手機為了便利以及輕薄設計，也帶來電量的限制，這都讓使用者需要攜帶行動電源或充電器，以維持手機的運作。針對此行為，駭客便利用使用者下載的漏洞，將病毒或惡意程式植入被害人手機中，當

被害人利用 USB 與電腦主機傳輸資料或是充電時，將惡意程式趁機入侵到電腦，並藉此突破原先可能採取實體隔離（沒有與一般民網連結）的電腦，甚至是其內部的網路系統。一般會採取實體隔離擁有「內網」的機關，必定是有相當機密性（如政府機關、軍方），因此一般都會禁止使用 USB 隨身碟作為資料儲存的工具;但許多單位卻忽略了利用 USB 充電所帶來的風險，特別是在近年駭客大會中，許多技術高超的資安研究人員都明確指出各種手機的漏洞，是有可能透過充電設備，與電腦形成交叉感染，並利用手機行動網路將原先在內網的資料傳送出去，導致資安防護網失效。

便利與隱私

對一般人而言，要嘗試監控自己手機是否被注入惡意程式或被定期回傳資訊有相當困難，甚至在安裝或傳送軟體的過程中，通常也不會注意到是否開放了部分權限供廠商運用；而這些都會導致消費者在不知情的狀況下，同意將資料交由廠商自由運用。有鑑於此，也有不少資安公司推出行動裝置安全防護的相關軟體，甚至針對不同系統的智慧型手機，設計出專屬的監控 APP 軟體，但這將導致用戶在使用 APP 時，必須對授權項目逐一勾選，也會造成使用者的麻煩；有人認為這些手機的防護軟體本身便不安全，沒有人知道這些公司背後是否有其他盤算，甚至藉此蒐集並建立更龐大的個資資料庫。

所謂資訊安全，都回歸到人類使用科技最初動機的便利性，曾有業者的廣告詞為「科技始終來自於人性」，資安風險也一樣，許多公私營單位雖然有許多規範，而使用者也願意配合，甚至選購資安產品服務（包含系統），但最後因為個人疏忽以及貪圖方便（如勾選授權、透過不明無線網路上網、傳輸重要資料並無加密習慣），都可能會讓原先在資安上的努力功虧一簣。畢竟資安不是產品，而是一個過程，也是組織裡每一分子都必須負起的責任。（文摘自法務部調查局清流月刊 104 年 1 月號）

嘉義區監理所 關心您