臺中市政府經濟發展局政風室

公務機密宣導專欄

行動應用 APP 資安威脅及案例

隨著 APP 數量以及使用者將機敏資訊存於行動裝置的比例增加，惡意 APP 對使用者的威脅以及損害程度逐漸上升。除了個人使用者外，企業同樣也遭受惡意 APP 的入侵，這些惡意 APP 可被分為以下五種類型：

一、廣告(Adware)：經常偽裝成一般合法應用程式，並涉及購買行為。

美國的移動安全防護及分析公司 Wandera，曾發現 Google Play 商店中的兩款美肌 APP 會跳出惡意廣告，並且加速行動裝置的電量流失。因此，當使用者下載行動應用 APP 後，若有廣告出現或是行動裝置的運行速度變慢，電池耗用增加，極可能是下載並遭到惡意 APP 的侵襲。

二、網路釣魚(Phishing)：此種類型之惡意 APP 主要是將使用者導入釣魚網站，並且誘導使用者輸入相關資訊，以竊取個人資料。趨勢科技發現在 Google Play 商店中，有多款美肌相機 APP 會將使用者導入釣魚網站中並使其留下個資。因此，若使用者在下載並安裝行動應用 APP 後，突然收到關於贏得獎品，或帳號、訂閱服務將被停止等訊息，都極有可能遭到網路釣魚 APP 的駭侵。

三、殭屍網路(Bots)：此種惡意 APP 可以在行動裝置後台運作，和殭屍控制主機(botmaster)聯繫並執行命令，使用者不易察覺。

曾有一款名為 Hidden Administrator 的惡意 APP，以 Android 系統為目標，在進入受害者行動裝置之後便隱藏起來。此應用程式會將自己的權限提升至管理員等級，並且控制該受害行動裝置，

臺中市政府經濟發展局
TAICHUNG CITY GOVERNMENT
ECONOMIC DEVELOPMENT BUREAU

創新 Innovation　服務 Service　活力 Dynamics

使變成殭屍網路或挖礦的工具。因此，若使用者在下載並安裝 APP 後，其行動裝置容易產生連線中斷、網路無法連接，或是在未經使用者授權的情況下，行動裝置自動安裝或移除任何 APP，則該行動裝置極有可能已下載到殭屍惡意 APP。

四、間諜軟體(Spyware)：會監控和記錄使用者的裝置狀態或行為資訊，例如簡訊、電子郵件、電話紀錄、聯絡人、地理位置等訊息，並分享給遠端的伺服器。

趨勢科技發現六款於 Google Play 商店上架之間諜軟體 APP。這六款惡意 APP，都是由被稱為「MobSTSPY」的間諜軟體偽裝而成，當使用者啟動後，間諜軟體會檢查行動裝置的網路狀態，搜集裝置型號等設備資訊，以及簡訊、電話簿等使用者資訊，再將竊取的資訊回傳給中繼站伺服器。因此，使用者在下載並安裝行動應用 APP 後，若發現行動裝置有奇怪的行為，除了應將可疑的 APP 移除外，也必須檢查內部是否有被安裝或放置可疑的檔案及程式，並將其移除和卸載。

五、下載器(Downloader)：此種程式自身並非惡意程式，但會隱身於 APP 中，負責下載其他的惡意程式到使用者行動裝置中。

以色列資安公司 Check Point，在 Google Play 商店中發現一款新的惡意 APP。該惡意 APP 具有開啟特定網址的功能，並進行網路釣魚行為，也能替受害行動裝置安裝新的惡意程式。因此，當使用者下載並安裝 APP 後，若出現未經使用者授權下載之 APP、檔案，或突增電池耗用、網路流量，以及額外費用等，都可能是行動裝置遭惡意下載器感染所致。

【資料來源】

☞ 臺中市政府政風處