木馬程式 Marcher 進化，假冒 Android 韌體更新、知名 App 程式及網頁

研究人員發現 Marcher 的散佈手法進化，假冒 Android 韌體更新，或是假冒 Viber、Gmail、Chrome、Intagram 等知名程式，跳出網頁騙取資料，C&C 通訊也從 HTTP 改為 SSL 加密，木馬也以 base64 編碼及字串取代功能躲避偵測。

文/林妍溱 | 2016-08-17 發表

示意圖，與新聞事件無關。

今年稍早資安業者Zscaler 揭露專門竊取資訊的木馬程式Marcher，如今該公司發現 Marcher 又再更進化，假冒成 Android 韌體更新程式，或是 Facebook Messenger、Gmail 等 App 網頁誘使用戶上鉤，而躲避追查的技術也更高。

Marcher 首度出現於 2013 年，鎖定 Google Play Store，等使用者開啟 Play Store App 時展示覆疊的 HTML 網頁，以霸佔螢幕的方式強迫使用者輸入信用卡資訊。後來 Marcher 又演化到冒充金融機構騙取用戶的信用卡資訊，範圍遍及德、澳、法、美、英國國及土耳其。

最近 Zscaler 發現 Marcher 在多方面都演化出更高明的技巧。首先，原本 Marcher 只透過假冒的 Amazon 及 Google Play Store app 散佈，但本月研究人員發現 Marcher 假冒 Android 韌體更新程式。它在用戶裝置植入 Firmware_Update.apk 的程式，顯示裝置有漏洞，為防遭病毒入侵竊取個人資訊，要求他們儘快安裝升級程式。而在安裝時，Marcher 會藉機要求使用者輸入管理員資訊。

另外，Marcher 假冒的 App 對象也愈來愈大膽；原本它只假冒 Google Play Store 資料輸入頁，研究人員在最近的樣本中觀察到它會用戶使用知名 App 時，包括 Viber、WhatsApp、Skype、Facebook

Messenger、Gmail、Chrome、Intagram、Twitter 和 Line 等等，也會跳出假冒的 HTML 網頁騙取用戶資料。

此外，研究人員也發現 Marcher 傳送竊取用戶及裝置資訊的 C&C 通訊，也從簡單的 HTTP 協定進階到加密的 SSL。這隻程式還會判斷用戶是否為俄羅斯獨立國協，如果是就會停止活動，顯示這隻木馬控制中心可能來自本地區。同時作者開始使用 base64 編碼及字串取代功能來混淆程式以躲避追查，這也是前所未見。

研究人員表示，Marcher 種種進化使它成為 Android 裝置散佈範圍最廣的威脅。為免受害，呼籲使用者僅從受信賴的應用程式商店如 Google Play 下載 App，也可從裝置上的「安全」設定取消勾選「不知名的來源」。

資料來源：iThome