超級木馬病毒

竊聽手機私隱

內地市面已有流傳 幾秒取通話短訊視像

《世界新聞報》竊聽醜聞引發軒然大波，幾乎人手一部的智能手機更接連爆出竊聽漏洞，用戶的私隱幾秒內便蕩然無存！香港文匯報記者近日從業內人士處獲悉，網上已出現針對iPhone和安卓（Android）系統的智能手機的竊聽木馬病毒。該病毒可以以電腦操作，暗中發送手機通用格式的信息到目標手機，當目標手機重新啟動，病毒立即進行安裝。隨後，發送者只要啟動程式，便可在不知不覺中將目標手機的通話、短訊、照片、視頻和位置等信息，甚至已刪除掉的記錄複製過來，時間僅需幾秒鐘。而且在此病毒面前，幾乎所有智能手機無一倖免。 ■香港文匯報記者 鄭海龍 深圳報道

隨着各類智能系統的手機越來越普遍，高科技電子產品在給人們享用方便快捷的科技成果的同時，個人信息安全風險也逐漸在增加。近日，有內地公司的註冊網站甚至公然在網上銷售類似病毒，使原本受控於某些政府部門在特定情況下才允許使用的「偵察」手法，變得垂手可得。或許，這樣的病毒，已經潛入了你的智能手機。

「加殼」掩飾避殺毒軟件

「一共才幾十Kb小，在手機的可執行性文件中算大的了，但是能力不小，我用兩台iPhone手機，500多個電話號碼，只用了幾秒鐘就被全部COPY（複製）出來了。」有業內人士向香港文匯報記者報料，稱這個病毒是他偶然在網上發現的，因為自己做軟件，就研究了一下。

他說，這個病毒本身有加殼現象，一般的手機殺毒軟件對這個病毒執行性文件無任何反應。當這個病毒在電腦安裝好之後，可以給任何一個號碼發送一個手機通用格式的短訊，而這個短訊會顯示為空白或者無法打開，這時即使立即將該信息刪除，病毒依然保留在手機系統中，只要手機重新開機，病毒就會自行安裝，並在目標手機徹底潛伏下來。

該人士稱，一旦安裝成功，被安裝了病毒的手機會給黑客回覆一個信息，黑客隨後就可以啟動這個病毒程式，將手機的通訊錄、通話、短訊、照片、視頻以及GPS位置等信息，統一以文件形式發送給黑客。

利用系統本身漏洞傳播

「最要命的是，這個病毒無法刪除，即使你重新裝了手機系統，它依然存在。就跟影子一樣。」該人士透露，實際上針對手機的類似間諜病毒，並不是第一次發現，而是隨着智能手機的普及，而逐漸形成了一個龐大的個人信息安全漏洞。他說，這個病毒利用的是智能手機系統本身的漏洞傳播，最後控制系統並隱藏運行，將手機變成潛藏在你身邊的間諜。

據了解，目前市面上流通的類似病毒，針對塞班、安卓、iPhone，甚至中國移動自己訂製的OPhone系統都已被染指。「其實我們可以了解，這是一個必然情況，畢竟潛在的商業市場龐大到了如此地步。這些個人資料隨時可以被當成商品銷售。」他說。

分析機主身份
伺機詐騙勒索

有供有求 電訊業人士接受香港文匯報記者採訪時表示，實際上任何一款所謂的病毒，背後都至少有一條黑色產業鏈，將各部分連結起來。而這些病毒從放出來開始，就存在惡意目的。就目前的手機病毒來看，大部分的手機病毒都是為了竊取手機的通訊記錄或聯繫人列表等。

該人士透露，一般內地的黑客，受僱傭後，往往到國外的相關網站和論壇尋找相關的黑客工具以及病毒腳本，然後再改寫成中文版，或進行本土化修改，再賣給買家。買家購買這些病毒，真正的用處主要在於分析整理潛在「客戶群」，通過電話號碼或通訊資料分析對方的身份等信息，然後研究好詐騙手法，有針對性地進行金融詐騙或勒索。

私家偵探是主要買家

業內人士透露，實際上，這些病毒的終端用戶很大一部分是私家偵探。「他們買下這些病毒，暗中安裝給目標手機，然後跟蹤位置竊聽內容以充證據，因此每個人都會有遇到的風險。」

■當智能手機接收到空白短訊時，重新開機之後，手機內的所有信息可能隨時遭竊取。 資料圖片

公開經營手機病毒 內地首截獲

無所顧忌 知名手機反病毒安全科技公司金山手機安全中心上月底截獲一款由商業公司經營的移動間諜手機後門程序。該程序的功能與主文的病毒功能相似，但未知這兩個病毒是否相同。這是內地首次截獲商業公司公開經營手機病毒。

「這是少有的公開經營手機病毒的行為，此前從未發現任何組織或個人公開製作銷售手機病毒。」金山手機安全專家說，「以前發現的手機病毒，是偷偷扣費，再把SP下發的確認短信刪除。而今天截獲的手機移動間諜後門程序（Android.Hack.SWMsgspy.a），卻在官方網站上聲稱要做中國最大的手機監控網。」

金山技術人員通過工信部ICP備案信息檢索發現，這個號稱中國最大手機監控網的站點ICP備案信息無異常，備案的公司名為「廈門市××數碼科技有限公司」，但與在廈門的企業黃頁上檢索到的信息並不完全吻合，目前尚不清楚這個經營手機病毒的公司是否真的存在。

先存機主通話 再傳往接收器

這個移動間諜手機病毒和前一段時間廣為人知的「手機×臥底」非常類似，而且經營者也自稱是手機×臥底，估計病毒作者只是想在搜索「手機×臥底」時，點擊到自己的網站。實際上，這兩個病毒區別明顯：手機×臥底病毒是利用多方通話功能竊聽，移動間諜手機病毒則和PC上的後門程序幾乎沒有差別。這證明隨着手機技術的發展，病毒也出現了換代，從扣費的流氓軟件，轉化成真正意義上的病毒。

據金山手機安全中心分析，上述公司經營的手機病毒程序可以將手機上的全部短訊轉發到指定的伺服器，將手機用戶的通話保存在手機存儲卡，通話結束後再上傳到指定的伺服器，從而使中毒手機的短信和通話完全被竊聽。

洩私隱 可導致金融詐騙

當中毒手機開啟GPS定位服務使用時，這個移動間諜手機病毒還會將準確的GPS定位信息和短訊記錄、通話錄音數據等一併上傳到伺服器，從而完全掌握中毒手機用戶的行蹤。當手機裡的關鍵私隱信息洩露，可能導致隨之而來的金融詐騙或其他嚴重損失。

金山手機安全專家建議網民不可因一時好奇，在手機上安裝類似的間諜軟件。而在下載軟件時，也要注意軟件中是否會被植入木馬，同時手機中要安裝殺毒軟件，定期進行查殺。

用家多缺警覺心：蘋果怎會有毒呢？

防範病毒 在這個智能手機「氾濫」的年代，智能手機已經集電腦、娛樂、資訊、私隱等種種與生活息息相關的關鍵詞於一身。但民眾對手機病毒的危害又知道多少呢？記者隨機採訪了6名手機使用者，只有一人表示，會小心選擇軟件安裝。對此，手機軟件工程師建議，用戶在使用智能手機下載軟件時，盡量選擇受驗證允許的軟件，同時在不需要的時候盡量關閉網絡連接及關閉GPS定位。

在記者的採訪中，多名女性是iPhone的忠實粉絲，而她們對於病毒問題的看法，大部分仍停留在幾年前的思維當中。「蘋果的系統怎麼可能有病毒呢？不是只有用Windows系統才會有病毒嗎？」

黃先生使用HTC手機已經多年，「我原來下載過手機防病毒軟件，但是不管我覺得我的手機是不是不好用了，也沒有辦法用防病毒軟件殺出病毒來。而且一年前下載的軟件，一年後升級都說是最新版本，感覺軟件是騙人的。」至於手機病毒一事，黃先生稱，有必要小心一下，否則可能給自己造成很大的影響，甚至陷入騙局。

「手機用多了，黑客才會研病毒」

對於黃先生的說法，有資深軟件工程師表示，以往的病毒主要集中在電腦的視窗系統之中，但隨着智能手機的逐步發展，病毒種族也逐漸開始壯大，以盜竊信息為主的病毒，開始向新的智能終端發展。「這是必然的趨勢，（智能手機）用得多了，黑客才會研究病毒出來盜取你的信息和資料銷售牟利，而之前手機防病毒軟件之所以一兩年都不用升級，完全是因為沒有人研究類似的病毒被我們監控到，因此也就不需要升級殺毒程序。」

專家：選受驗證允許軟件

該軟件工程師並表示，實際上防護病毒最好的方法並不是被動防禦，而是主動將病毒載體拒之門外。用戶在使用智能手機下載軟件時，盡量選擇受驗證允許的軟件，減少病毒偽裝成軟件混進手機系統中的機會，同時在不需要的時候盡量關閉網絡連接及關閉GPS定位。

版面導讀

要聞 大運會帶旺 港酒店住客料升
港旅遊界估計，即將開幕的深圳大學生運動會將為香港帶來新客源，本月下旬入住率會不跌反升一成。 詳刊A6

要聞 廣深通高鐵 5車站就緒
廣深高鐵開通在即，記者採訪沿線5個車站，發現主體建設及設備裝配已經完成，正在進行站點外圍修整。 詳刊A7

中國 中方駁英報「脫軌論」偏頗
中國駐英使館駁英國《每日電訊報》，指該報借一件事故否定中國鐵路建設，預言中國經濟也將脫軌的評論偏頗。 詳刊A9

港聞 男嬰獨睡翻身 墮污衣籃險焗死
旺角廣東道一名六個月大男嬰，疑熟睡期間翻身跌進床邊的污衣膠籃內被掩埋，其父母發現後送院急救。 詳刊A16

娛樂 港姐決賽 朱晨麗大熱勝出
《2011香港小姐競選決賽》昨晚舉行，賽前大熱門5號朱晨麗摘后冠，亞軍則爆冷由14號朱希敏奪得。 詳刊A17

國際 警察槍殺男子 引發倫敦暴亂
英國倫敦北部托特納姆前晚有逾500人在警局外聚集，抗議警方上周無故槍殺一名男子。示威後演變成騷亂。 詳刊A20