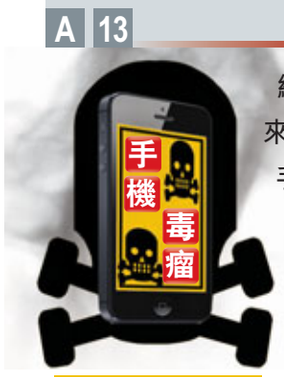


系列專題 二之一

內地手機病毒肆虐 狂吞港人漫遊費

暗藏龐大黑色產業鏈 每日暴利達千萬

■內地成為手機病毒重災區，而病毒更已蔓延香港。 資料圖片

編者按：智能手機瘋魔全球，人們在享受各式軟件帶來的便捷和趣味時，可有想過在夜深人靜、您關閉手機顯示器時，甚至在打電話、玩遊戲、聽音樂時，您的手機可能正被千里之外的陌生人操縱？您的通話記錄、短信及私隱可能被竊聽？您的朋友可能收到「您」發出的病毒短信？您的通話費也因此被悄悄偷走？只因您的手機中毒了！

根據調查，2012年三季度全球共查殺到手機惡意軟件23,375款，中毒智能手機近千萬部，中國大陸成為重災區，而病毒更已蔓延香港！本報為此推出「手機毒瘤」系列專題，透過採訪通信業人士，剖析手機病毒氾濫情況，背後產業鏈運作及利益分攤，提出解毒方案，及用戶防毒清毒招法。

隨着智能手機的普及，內地各種花樣的手機病毒大肆傳播，惡意扣費、竊取私隱等行為日益猖獗。一些以感染香港用戶為目的的含病毒軟件也在香港論壇出現，黑客對準兩地運營商間的接駁漏洞實施攻擊，狂扣港人漫遊費。手機產業生態的幾乎所有環節，包括山寨手機生產商、軟件開發商、通信增值服務提供商(SP)、流動網絡商等都或多或少地被捲入這條「手機黑金」利益鏈。業內人士稱，僅一款暗扣話費的惡意代碼，每年直接偷偷暗扣手機用戶的話費總額就超過5,000萬元；僅一天內，通過「遠程控制木馬」進行惡意推廣的最高獲利或達千萬元。病毒產業鏈龐大，服務提供商和流動網絡商扮演角色重之又重。

■香港文匯報記者 鄭海龍、李薇 深圳報道

病毒擴散月增7倍 中國成重災區

手機防病毒軟件公司——北京網秦天下科技有限公司發佈的《2012年第三季度全球手機安全報告》指出，「雲安全」監測平台在2012年三季度共查殺到手機惡意軟件23,375款，環比增長92.7%，查殺款數超過2012年上半年總和（17,676款）。三季度感染惡意軟件的智能手機總計991萬部，環比增長30.3%。數據顯示，中國大陸地區以25.7%的感染比例再次成為全球最大重災區，其中，廣東省以22.5%的受災率居首。

而Android（安卓）平台已完全成為惡意軟件的重點感染對象，78%的惡意軟件來自Android平台，多偽裝為主題類、工具類和電子書App應用進行傳播。同時，手機論壇以27.3%的感染比例成為惡意軟件的主要傳播途徑，業內專家指出，目前網上近三成的「刷機包」（港稱Root機）都蘊含安全隱患，暗藏流氓推廣軟件和惡意扣費軟件。

對此，公安部微博「公安部打四黑除四害」，上月中旬也發佈相關預警，稱Android系統手機上，惡意軟件正在以每月800%(月增7倍)的速度快速增加。

小科技公司成幫兇

■深圳華強北聚集大量家庭式科技作坊。

作為深圳的科技支柱產業，手機及周邊產業則是深圳出口型經濟的主要代表。國產的手機以往因系統簡陋，材質差而被稱為「山寨」貨。作為智能手機的主要「核心靈魂」的系統，在無序的國產手機市場環境下也被覬覦着。不少科技公司以修改系統，並將以前MTK（國產山寨手機系統）手機所使用的「鉤子程序」代入其中為生。而這些「鉤子程序」最主要的作用即為扣費。

在深圳的科技園區乃至華強北的家庭作坊，往往三四個人幾台電腦，外加一個工程塑料製作的公司標牌，即可成立一家科技公司。方先生的公司即是這樣的規模。

方先生的公司主要負責手機組裝。「一般來說，國產的比較大的品牌，會購買一些系統，一般系統軟件開發公司，會在Google上尋找Android的開放源代碼，按照要求訂製改造智能系統。而對於一些小品牌或者是高仿機，這些公司一般都會選擇零價格出讓系統。」

系統研發商「下鉤」

方先生介紹，所謂的零價格是指科技公司將系統無償發給手機組裝商使用。但這裡的系統大部分是經過改裝的，裡面多少會有扣費的程序。這些程序甚至直接寫進系統中而不被使用者發覺或消除。

「這些做法實際上是系統研發商沿用了傳統的MTK系統手機，換法子使用『鉤子程序』。」方先生稱，這些下「鉤子程序」的系統開發公司，一般是兩面拿錢，「一邊是程序方的『下鉤』錢，一邊是鉤子程序的扣費收益分紅。」

P小姐在香港一家貿易公司工作，由於工作關係，需要經常往返兩地。不久前她到深圳公幹，不出一個禮拜，漫遊上網費竟要兩千多元！

下載遊戲失二千元

「要知道我的電話費由信用卡即時過數，臨急臨忙惟有打電話到香港流動網絡商，他們首先說我的手機確實在內地期間產生巨額的上網流量，如果有疑問需找內地的移動電話公司，等我找到內地的移動電話公司時，對方又搬出另一套話，最後因我無法拿出他們所需證據，只能不了了之。」話費追不回，P小姐向手機達人查詢，最終發現自己的手機原來中毒，病毒來自她曾在論壇上下載的一個小遊戲，以至手機在「後台」私自下載，消耗手機流量。

有業內人士稱，一些以香港用戶為主要目標的含病毒軟件已在香港的智能手機論壇及下載渠道散播。這些軟件主要吃準兩地網絡商間的接駁漏洞進行攻擊，與此同時，大部分香港手機用戶一般用信用卡支費，也引起內地黑客公司覬覦。

無獨有偶，中國公安部微博公佈的案例稱，廣東黃先生前陣子因買了部帶有惡意軟件的手機，一個月竟然不見了40多萬話費！記者一名在深圳經營手機生意的朋友、港人方先生也遇到類似情況。

病毒觸發 悄悄扣費

北京網秦公司手機防病毒專家劉晶晶接受記者採訪時表示，目前感染規模比較大的智能手機病毒，主要以食人魚、吸費蝙蝠及安卓吸費王為主。這些病毒被黑客寫進正常應用軟件腳本，以致應用軟件成為特洛伊木馬潛伏在手機中，並伺機扣費。「這些病毒被觸發後，一般會悄悄進行扣費，額度在兩到十元不等，而按照上季度相關數據計算，這些以扣費和資費消耗為主要危害的病毒，今年一季度『產值』至少在300萬到1,740萬之間。而這個數據也在跟着惡意軟件的激增而迅速膨脹。」

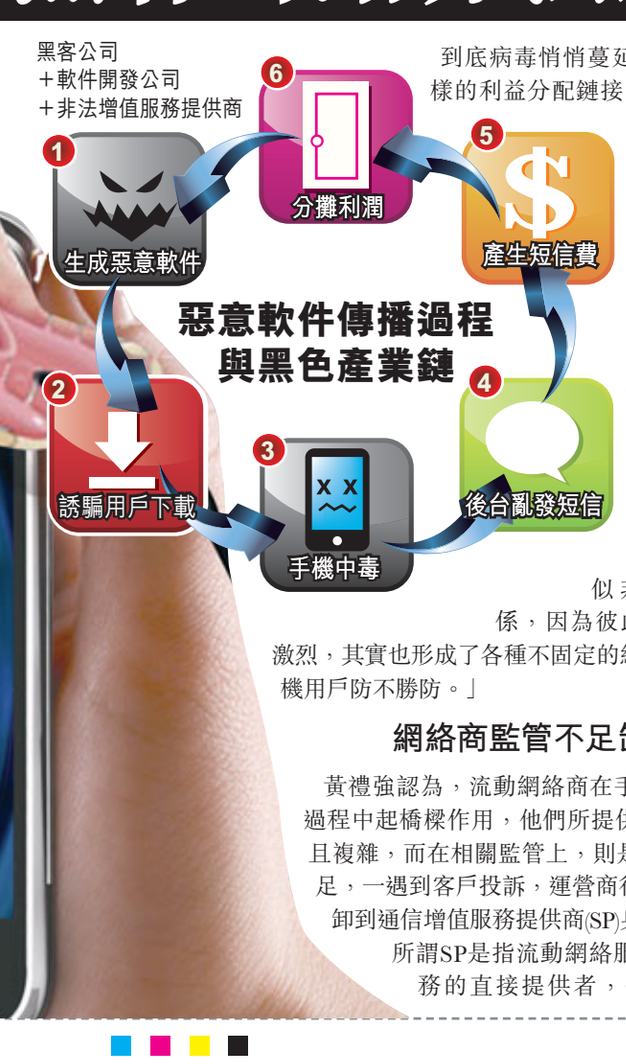
軟件權限日益擴大

實際上，只要稍微注意一下智能軟件在手機中的安裝過程，即可輕易地發現這些軟件在安裝時都向用戶索要哪些權限，「比如，接打電話、發送短信、GPS定位、甚至調取通訊錄、通訊記錄、照片視頻等等，這些權限，一旦用戶選擇同意授權，即意味着這些軟件隨時可在後台執行上述內容，而不再告知用戶。這也是為什麼總是有一些廣告可以精準投遞到社會精英人士的手機上的其中一個途徑的原因。」業內人士指出。

開發智能手機軟件的行業准入門檻非常低，甚至不需要任何行政審批，因此這些軟件在開發之初的源代碼（Source code）時期，就帶着創作者的功利性。「只要寫這個程序的人願意，這個程序就可以有任何功能，只要不是太出格，就不用擔心有行政部門的干預。」

因此扣費、吸金、甚至垃圾廣告投放，都在智能手機中，借助軟件的應用得以施展。而對象，不僅僅包含源代碼開放的Android系統的智能手機，還包括Symbian以及越獄的iPhone系統。

黑客勾結非法服務提供商吸金



到底病毒悄悄蔓延的背後存在怎樣的利益分配鏈接？360手機安全專家黃禮強告訴記者，一個手機病毒要從用戶手機上獲取利潤需經5個環節，分別為：研發、與非正規站點合作傳播、用戶、向流動網絡商訂製扣費服務，以及與計費點公司合作。「這些看似非常牢靠的關係，因為彼此之間『競爭』激烈，其實也形成了各種不固定的組合搭配，讓手機用戶防不勝防。」

網絡商監管不足卸責

黃禮強認為，流動網絡商在手機病毒傳播的過程中起橋樑作用，他們所提供的增值業務多且複雜，而在相關監管上，則是明顯的力度不足，一遇到客戶投訴，運營商很輕易將責任推卸到通信增值服務提供商(SP)身上。

所謂SP是指流動網絡服務內容應用服務的直接提供者，合法SP有手機QQ、搜狐、新浪、網易、中華網、Tom等。SP通過流動網絡商提供的增值接口為用戶提供服務，然後由網絡商在用戶的手機費和寬帶費中扣除相關服務費，最後網絡商和SP再按照比例分帳。

據網秦手機安全專家劉晶晶介紹，手機病毒的黑色產業鏈的吸金模式主要是：黑客公司通過和軟件開發公司、手機增值服務公司（通常是非法）互相勾結，或將一些惡意代碼植入知名手機軟件中，或將扣費病毒偽裝成一些用戶日常需要的軟件。當客戶手機被這些病毒所感染，病毒就會通過惡意扣費和竊取用戶隱私贏利。「就惡意扣費來說，一般機主每月都被扣2元-10元，由於扣費金額較小，加上木馬病毒會主動屏蔽或刪除扣費信息，因此機主很難察覺。」劉晶晶稱。

黑客公司獲利至少三成

在這5個環節當中，黑客公司需支付非正規網站、流動網絡商和計費點公司一筆為數不小的費用。據黃禮強介紹，一個病毒一般生存周期為3個月，如果以5萬個手機用戶每個月被扣取2元手機費計算，一個病毒在一個生存周期內至少可獲利30萬以上，而黑客公司在其中獲取利潤最少也有3成。其餘的7成則用於支付其他環節的費用。

據「江湖規矩」，假定一個用戶被悄悄扣了10元信息費，流動網絡商首先要拿走1.5元的通道分成，並會根據實際情況扣除一定比例的壞賬，一般SP和CP（內容提供商）能拿到手的分成為7-8元。其後，按照行規，SP和CP能從中拿走30%，剩餘70%由手機廠商和方案廠商對半分成。