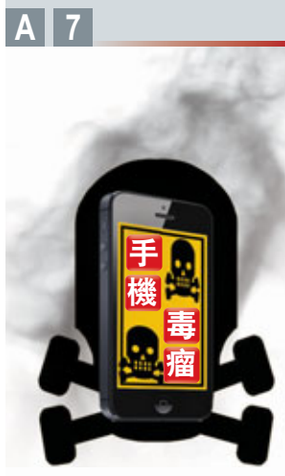
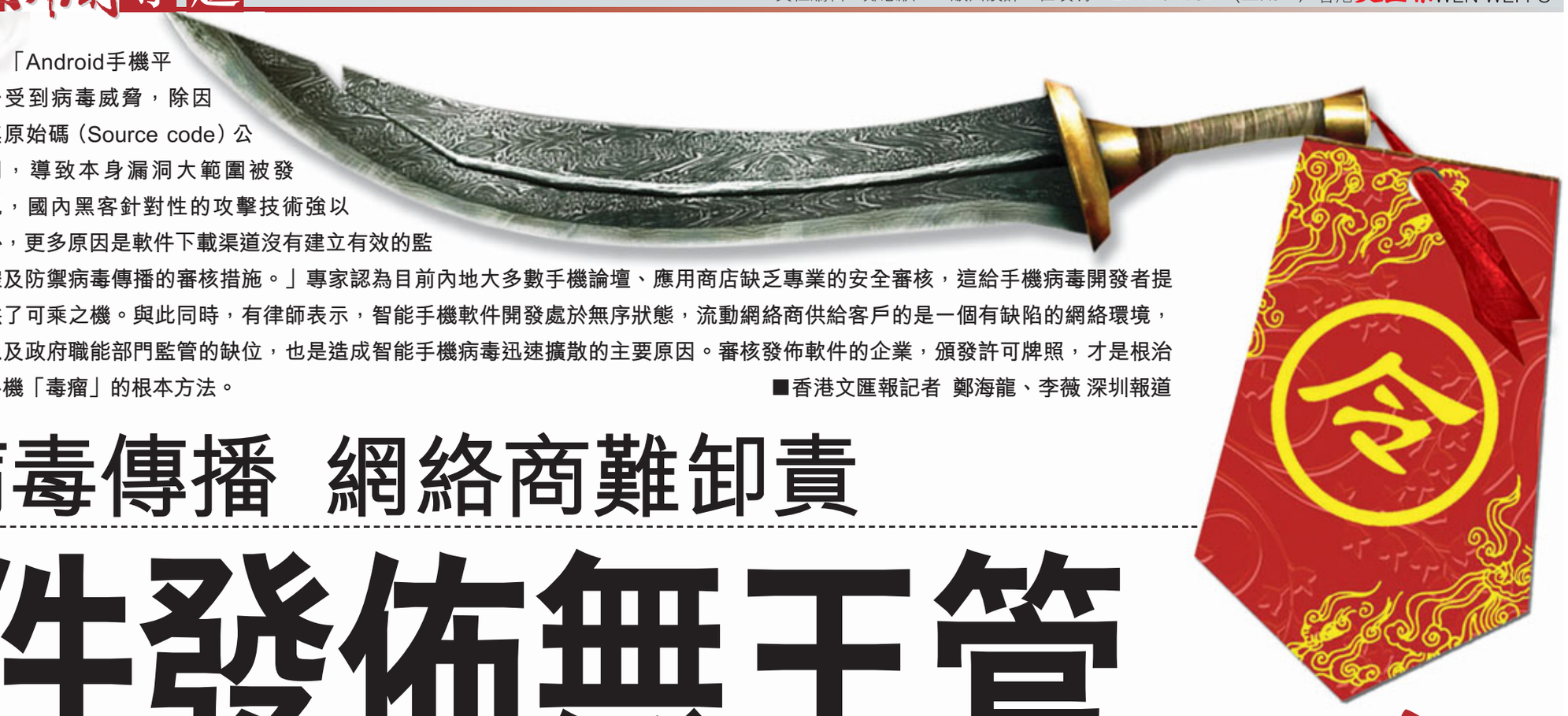


系列專題 二之二

「Android手機平台受到病毒威脅，除因其原始碼（Source code）公開，導致本身漏洞大範圍被發現，國內黑客針對性的攻擊技術強以外，更多原因是軟件下載渠道沒有建立有效的監控及防禦病毒傳播的審核措施。」專家認為目前內地大多數手機論壇、應用商店缺乏專業的安全審核，這給手機病毒開發者提供了可乘之機。與此同時，有律師表示，智能手機軟件開發處於無序狀態，流動網絡商供給客戶的是一個有缺陷的網絡環境，以及政府職能部門監管的缺位，也是造成智能手機病毒迅速擴散的主要原因。審核發佈軟件的企業，頒發許可牌照，才是根治手機「毒瘤」的根本方法。

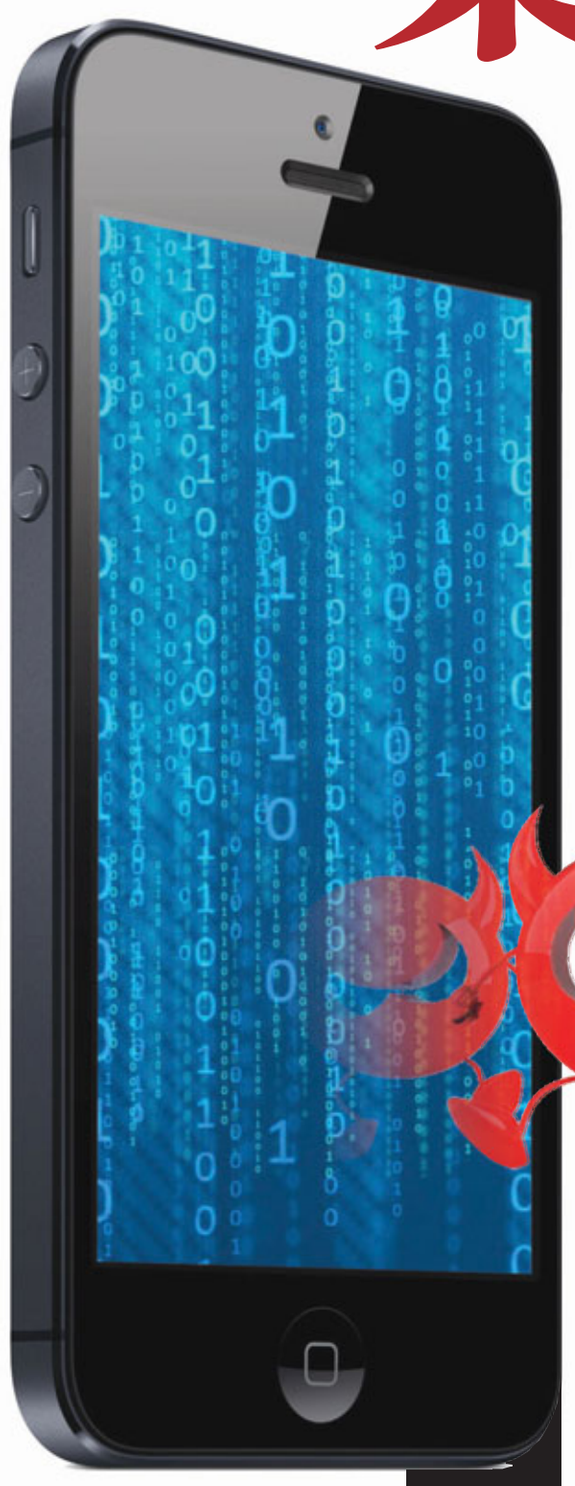
■香港文匯報記者 鄭海龍、李薇 深圳報道



默許病毒傳播 網絡商難卸責

軟件發佈無王管

業界籲發牌殺毒



北京網泰公司手機防治病毒專家劉晶晶認為，由於Android系統沒有如Symbian系統（早年Nokia智能手機使用系統）的第三方簽名認證機制，這給用戶安裝文件帶來方便的同時，也給獨立開發者提供便利。但是，系統開放性越強，漏洞也就越大，開放性使Android系統應用中置入後門程序（指那些繞過安全性控制而獲取對程序或系統訪問權的程序方法）變得更為容易，日益猖獗的各式手機病毒正是建立在這樣的基礎上而飛速發展傳播。

綠色客戶端審核粗疏

目前Android系統手機比較常用的軟件應用商店主要是「豌豆夾」、「91手機助手」、「360手機助手」等，而一些專業論壇發佈的軟件也作為Android系統手機常用軟件的補充。「但是這些站點發佈軟件相當容易，簡單到只需要註冊，甚至不需要對軟件安全進行任何安全審核。

有的黑客公司看到這個漏洞，往往選擇下載量比較大的官方綠色客戶端，植入病毒後，再上傳上述渠道供人下載以為己牟利。」劉晶晶稱，現時的手機軟件市場管理混亂，且缺乏有效的法規進行約束，因此可以預見，智能手機病毒將會呈現爆發態勢。

廣東深大地律師事務所歐陽莉娜律師接受記者採訪時表示，智能手機病毒擴散的迅速，與其說是行業自律的不足造成，不如說是政府職能部門的監管缺位導致。」一個行業的規則不能只依仗行業自律完成，必須有政府部門介入監管。審核發佈軟件的企業，頒發許可牌照，用法律的手段約束企業及行業進行自我淨化，才是根治手機「毒瘤」的根本方法。

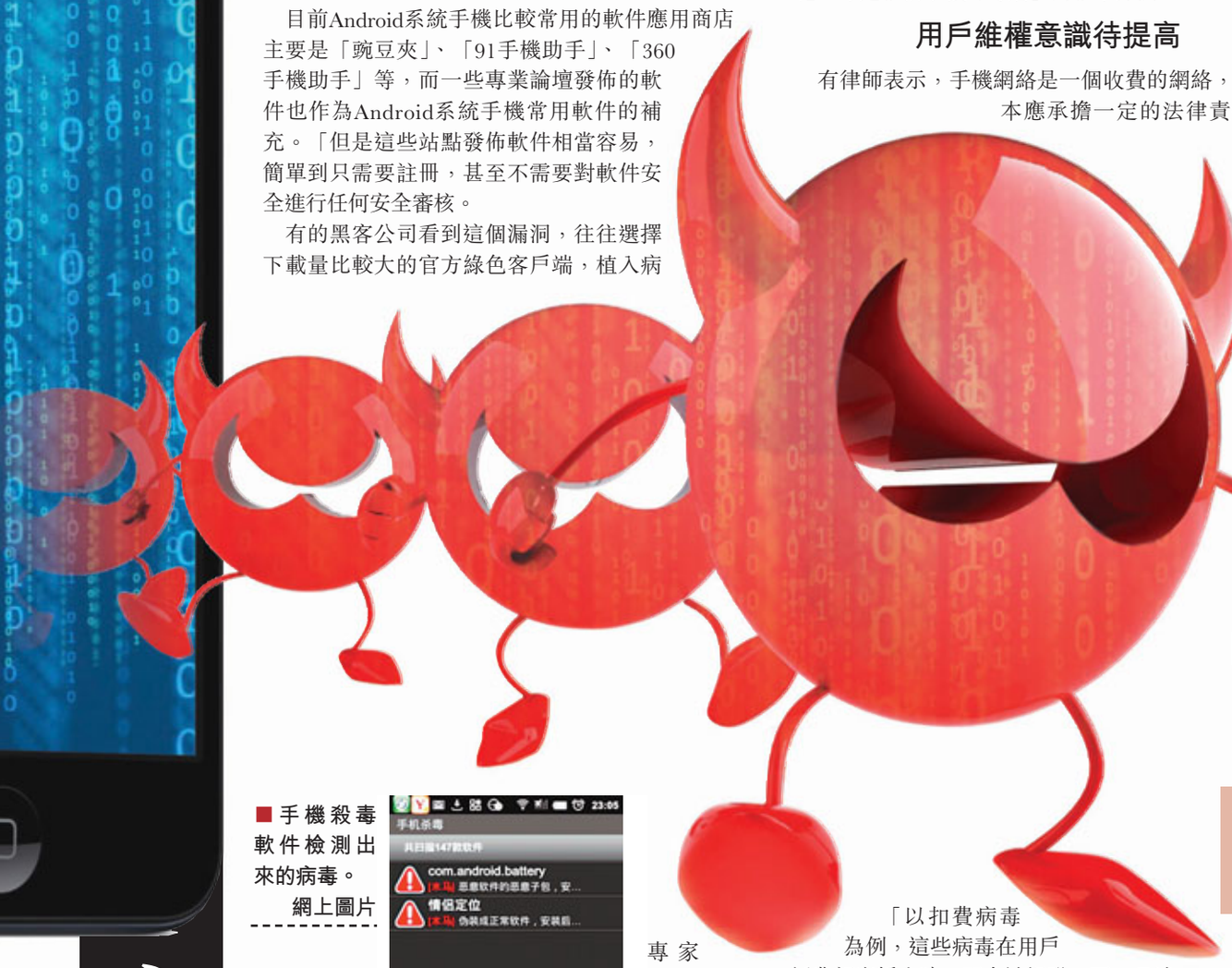
用戶維權意識待提高

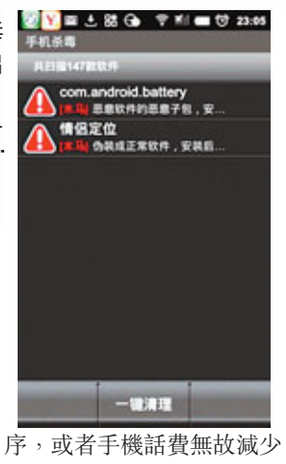
有律師表示，手機網絡是一個收費的網絡，收費者本應承擔一定的法律責任與義務。但中國移動、中國聯通及中國電信等企業在用戶手機費用被病毒吸走這個事件，起到的是紐帶橋樑的作用，甚至默許了這樣惡意的行為，那麼他們本身也是受益者。因此該律師呼籲遇到類似的事情不能僅僅要回話費就當沒發生，還要有用戶有維權的意識。

一般情況下，用戶手機中毒了，部分人選擇自認倒霉，部分人選擇拿起電話到流動網絡商處投訴要回那些被病毒吸走的話費，「但是單個客戶如果損失較小，舉證上是比較有難度的，因此很多人選擇了沉默。」360手機安全專家黃禮強說。

有深圳律師表示，倘若中國移動、中國聯通提供給客戶的是一個有缺陷的網絡環境，在客戶利益受損的情況下，他們未能給予任何的幫助，那麼他們不僅沒有商業道德，更涉嫌對客戶造成民事侵權。有維權意識的用戶和律師應該用法律武器維護權益，至少也是對法律環境的維護。

■一名正在聽電話的男子在中聯通門市前走過。 資料圖片





■手機殺毒軟件檢測出來的病毒。 網上圖片

「以扣費病毒為例，這些病毒在用戶話費額度偏小時，不會被觸發。而一旦達到黑客設定的點，則開始暗中小量多次地進行扣費，因為大部分人不會每天去查自己的電話費，也就不知道病毒的存在。這些病毒的隱匿性極強，很難被用戶發現。」劉晶晶稱。

盜取隱私 20萬手機受感染

此外，智能手機中竊取隱私的病毒，也佔有非常大的比重。網秦在發佈的《2012年第一季度全球Android手機安全報告》中指出，有超過30%的惡意軟件存在盜取隱私的能力。2011年下半年，網秦「雲安全」監測平台曾截獲一款名為「竊聽貓」惡意軟件，這款軟件當時在網上的售價為68元人民幣，購買者在完成支付以後，黑客公司會將該竊聽軟件偽裝成某款熱門遊戲，通過短信鏈接形式發送到用戶手機中，用戶一旦點擊鏈接病毒便會植入手機，購買者可全程監聽用戶的手機通話記錄，這一現象直接導致用戶關鍵隱私洩露。數據顯示，累計受該病毒感染手機超過20萬部以上。

由於在中國，手機的使用尚且屬於起步階段，以智能手機目前的數字處理能力來看(容量和運算)，還不至於強大到可以獨立處理、傳播病毒，所以病毒只能通過電腦、WAP服務器、WAP網關等平台來騷擾手機。客戶只要不接亂碼電話，盡量少從網上下載信息就不會有手機中毒等問題發生。

病毒「智能化」 中招難察覺

專家提醒，如果您的手機經常性的處於聯網狀態、無故自動下載並且安裝了應用程序，或者手機話費無故減少，甚至出現欠費停機現象，就必須警惕是否手機已經遭到惡意軟件的侵襲。

不過，網秦手機安全專家劉晶晶表示，現在的病毒隱蔽性越來越強，在前端很難發現病毒的痕跡。而其功能、形態的變化也讓技術人員有些措手不及。針對智能手機的病毒開始呈現智能化趨勢，令防病毒專家以及中毒者防不勝防。

識別地理位置 小量多次扣費

據業內人士稱，從去年開始，手機惡意軟件開始向地域性延伸，針對性的在不同地區推送惡意軟件，或借助計費通道來直接引導當地的受感染手機訂購當地的SP業務，增大訂購成功的機率。同時，這些智能手機病毒不僅可以智能識別手機的地理位置，根據用戶所在位置向不同地區的運營商發送短信扣取費用，還可能掌控用戶手機話費情況，在話費較少的時候病毒不會執行扣費，以避免被用戶察覺。一旦用戶充值了話費，這些病毒便有可能在半夜時間段多次扣除小額度話費，惡意扣費行為如此隱蔽，用戶便很難察覺。

小貼士 3招免毒

1. 必須安裝有效查殺病毒軟件；
2. 盡量選擇專業商店下載軟件，譬如手機廠商官網和中移動官網等，切忌在網上盲目搜索軟件；
3. 假若收到一些含有鏈接的短信或含有附件的彩信，不要輕易點擊，如果非得點擊不可，前提是已安裝有一些專業手機查殺軟件。而在安裝軟件時，要小心辨別軟件所需獲取權限，對於一些明顯不合理的權限要求，還是不安裝較好。

小貼士 3招殺毒

1. 安裝某些手機惡意軟件查殺工具進行病毒查殺；
2. 自行刪除帶有病毒的短信，在發現怪異短信時應立即關機，取下電池，將SIM卡取出並插入另一型號的手機中（手機品牌最好不一樣），將存於SIM卡中的可疑短信刪除後，重新將卡插回原手機；
3. 如果仍然無法使用，則應該與手機服務商聯繫，通過無線網站對手機進行殺毒，或通過手機的IC接入口或紅外傳輸接口進行殺毒。

八大常見手機病毒

病毒名稱	常見依附軟件	病毒殺傷力
1、CCa.tx.A 天下系列	天下寵物，天下社區等	會私自對外發送一條註冊短信，短信內容包含IMSI以及渠道標識，用戶毫不知情下，造成資費消耗；
2、MLC.gy.A 至酷壁紙系列	萬花筒動態壁紙，星系動態壁紙，聖誕節動態壁紙等	私自對外向多個號碼發送大量短信，惡意消耗資費；
3、CCRa.A	動感美女壁紙，海賊王精彩拼圖，性感車模看看等	私自創建其推廣軟件下載鏈接的桌面快捷方式，並私自聯網下載安裝，誤導用戶下載安裝，造成資費消耗；
4、MDa.mj.A	3D炫動魔方，iCalendar等	私自發送短信訂製SP業務，屏蔽運營商回執過來的短信，惡意訂製付費業務，造成資費消耗；
5、MDRa.kj.A 萬閱公寓系列	金屋藏嬌，攜美江湖行，絕代兵痞等	私自定製SP業務，聯網下載惡意指令，進行惡意扣費；
6、PSCa.sb.A	搶佔海島，細胞大戰等	電話信號強度，電量變化，開機自啟三個廣播接收後啟動服務UpdateService，嘗試獲取ROOT權限，私自下載並安裝流氓軟件，消耗用戶的手機流量，竊取用戶的隱私資料；
7、MSP.lx.C	冷血狙擊，坦克大戰，瘋狂騎士，極品美女等	開機自啟，短信電話監控，電話狀態改變，打出電話接收到四個廣播後啟動服務zjService，之後私自聯網下載流氓軟件，安裝流氓軟件，竊取用戶的短信內容和通話記錄以及手機信息，通過聯網上傳到木馬服務器；
8、PSCa.ed.A	鑽石迷情，拉燈，瘋狂打地鼠，掃雷等	電話信號強度，電量變化，開機自啟三個廣播接收後啟動服務UpdateService，嘗試獲取ROOT權限，私自下載並安裝流氓軟件，消耗用戶的手機流量，竊取隱私(手機串號等)