多為遊戲 日耗2GB數據 騙廣告客戶費用

apps隱形廣告 綁架手機「篤數」

■惡意廣告導致手機運作變慢，並消耗大量電源，教用家防不勝防。 資料圖片

有否發覺手機運作愈來愈慢？小心這可能是遭惡意廣告「綁架」！偵測網上廣告欺詐行為的Forensiq公司研究指出，超過5,000個包括遊戲等的應用程式(apps)暗藏惡意廣告，它們不是手機用戶一般可見到的廣告，而是在背景暗中不斷運行，騙取廣告公司的費用。同時，受影響的行動裝置每天被這些「隱形廣告」佔去最多2GB數據流量，導致運作變慢，並消耗大量電源，教人防不勝防。

Forensiq發表最新調查報告，指這種「行動裝置綁架」(mobile device hijacking)愈趨普遍，目前逾5,000個應用apps暗藏欺詐廣告，有1,200萬部行動裝置遭「綁架」，當中美國有1%的裝置中招，歐洲和亞洲較嚴重，有2%至3%。

廣告1拖10 從未開照出事

與其他惡意程式不同，含欺詐廣告的apps多為簡單的遊戲和手機工具，大部分可在蘋果公司和Android的官方app商店下載，部分更獲正面評價，深受用家信賴。這些apps多會搭配其他可疑的許可要求，像在開機時執行、避免裝置休眠、更改與刪除SD卡中的資料，或是在背景運作時仍能存取等。用家看到一個廣告的同時，可能有5至10個看不到的廣告在裝置的背景運行，有部分apps即使被用家關掉或從未開啟，亦會持續載入廣告。

助微軟可樂賣廣告 被下架

報告沒公開「綁架apps」的名稱，但彭博通訊社報道，製作Vampire Doctor和Celebrity Baby等Android遊戲的開發商「Girls Games Only」可能是其中之一。有用家投訴該公司的apps導致手機變慢和當機，Forensiq的影片亦顯示，相關apps編碼持續載入微軟和可口可樂等公司的「隱形廣告」。Girls Games Only沒回應事件，公司開發的apps周四已被Google Play下架。

Forensiq發現，受影響的裝置背景每分鐘最多載入20個「隱形廣告」，由於用戶看不到它們，故對廣告客戶而言毫無效益，但程式開發商仍可按載入量收取費用，變相構成詐騙行為。

全球廣告客戶年損失78億

手機廣告每1,000次點擊便有1至1.25美元(約7.75至9.7港元)收入，Forensiq估計廣告客戶今年約有13.3%、相當於8.57億美元(約66.4億港元)開支被欺詐廣告騙走。隨着需求增加和收費上升，今年全球廣告客戶可能因此損失逾10億美元(約77.5億港元)。

■彭博通訊社/《每日郵報》/《華爾街日報》/英國《金融時報》

惡意廣告流量比較 (30天觀察所得數據)

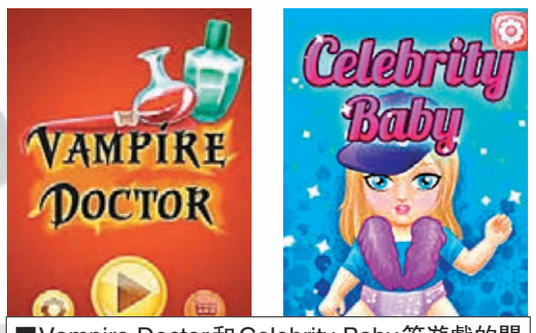
操作平台	apps總數	含欺詐程式apps	欺詐apps比率	流量分佈
Google Android	10,503	2,857	27.2%	54.7%
蘋果iOS	9,007	900	10%	42.6%
微軟Windows Mobile	15,733	1,404	8.9%	2.7%
總計	35,243	5,161	14.6%	100%

■資料來源：Forensiq

廣告客戶今年預計損失(以港元計)

操作平台	每千次點擊費用	估計損失
Google Android	7.75	37.2億
蘋果iOS	9.69	28.1億
微軟Windows Mobile	7.75	1.1億
總計	–	66.4億

■來源：Forensiq



■Vampire Doctor和Celebrity Baby等遊戲的開發商懷疑涉及「綁架apps」。 網上圖片

■惡意程式消耗數據流量，更載入微軟的「隱形廣告」。 網上圖片

殭屍程式扮真人 1/4瀏覽量呃錢

很多網上廣告以點擊率計算收費，令不法分子有機可乘，利用「殭屍程式」等手段推高點擊率，從而騙取廣告費。美國全國廣告商協會(ANA)和網絡安全研究公司White Ops一份研究報告指出，接近1/4的網上影片廣告瀏覽量是由欺詐程式偽造，而非真人觀看。

驗證碼公司Solve Media總裁雅各比表示，類似的欺詐問題日益嚴重，製造虛假點擊率的黑客不但技術高超，且非常小心，以免自己被捕。由於這種詐騙方式獲利頗豐，故吸引愈來愈多人投身其中。

廣告商近年雖然積極打擊詐騙，但問題始終無法根絕。廣告驗證公司Integral Ad Science總裁諾爾表示，這類廣告詐騙好像貓捉老鼠的遊戲，永遠都不會消失。此外，瀏覽量提高有助廣告商的宣傳計劃達標，賺取更多收入，故往往對這類欺詐行為「隻眼開隻眼閉」。

■《福布斯》/BusinessInsider網站/美國全國廣告商協會

參考用家評價 留心許可要求

現時的防毒軟件普遍無法偵測「綁架」手機的惡意廣告程式，因為它們的編碼非常混亂，難以確定哪個編碼導致不斷有廣告載入。Forensiq總裁森德羅夫教路，指一般而言獲高評價的apps安全較有保證，下載應用程式(apps)前，應先瀏覽其他的用家評價，若發現很多人投訴「食電」嚴重和令手機變慢，這些apps便很可能有問題。用家亦應定期查看手機，是否有程式用了過多數據流量。

森德羅夫又指，若apps提出可疑的許可要求，如開機運行或在背景運作時仍能存取等，用家便要提高警覺。若某些apps不需上網也能運作（例如單機遊戲），就應關閉apps網絡連線選項，防止暗中載入廣告。有些惡意apps即使重新開機，仍會自動在背景運作，因此用家應定期刪除較少用的程式。Forensiq指，有些「綁架apps」透過廣告交換平台隱藏真正身份，並假冒成Wickr和BBM等合法即時通訊程式。

美國加州大學戴維斯分校去年一項研究顯示，30%的Android apps在背景運行時會推送廣告，研究員更發現有27個apps在沒有按鍵的情況下，自動載入廣告。

■《福布斯》

港專家：避破解安全設定 免自毀長城

香港文匯報訊（記者 陳敏婷、郭兆東）手機應用程式暗藏惡意廣告，對每日機不離手的港人而言，是否難逃一劫？香港互動市務商會會長方保僑指，不少惡意程式會假扮為一般應用程式如遊戲及工具，要求存取不必要的權限及私隱資料，市民要自保，應避免自毀長城破解手機的安全設定。香港互聯網協會主席宋德嘉則指Android保安程度較低，較易出現問題。

■周先生 林嘉敏 攝

■黎小姐（右） 林嘉敏 攝

■張同學 林嘉敏 攝

程式賣私隱牟利 植入木馬

方保僑表示，智能手機惡意應用程式存在已久，花款更是多不勝數，當用戶安裝應用程式時，就會要求存取不必要的權限及私隱資料，例如位置、聯絡簿、鏡頭及咪高峰等，多數為了轉賣聯絡人資料牟利，更可藉此入侵用戶手機，植入木馬程式及電腦病毒，甚至偷取個人資料等。

他指出，部分遊戲本身要錢，但網上充斥所謂的「破解版」供下載，有關程式往往成為不法分子的入侵渠道，用戶因此而中毒的個案亦相當普遍。市民要自保，絕不應破解手機的安全設定，即是蘋果手機別「jailbreak」，Android手機則別「root機」。他提醒用家，下載應用程式前必須先留意程式索取的手機權限，強調「無理由一個電筒app會拿你的聯絡簿」。

Android保安程度較低

針對是次報道指惡意程式會強制彈出大量廣告，甚至在背景繼續運作而不為人知，方保僑指拖慢手機速度因人而異，視乎手機型號，但因此消耗大量數據是必然的事。

香港互聯網協會主席宋德嘉同樣擔心惡意應用程式衍生的私隱問題。他指出，Android的保安程度較低，向用戶索取存取權限時使用「all or nothing」的原則，用戶只可選擇交出權限然後下載，或是不下載，反而蘋果的IOS系統會逐項索取權限，亦會先仔細審批手機應用程式才於平台上推出。

他又透露，雖然Android聲稱今年底會推出新的系統，仿傚IOS系統逐項索取權限，但他日前與Android的首席人員傾談後，對方仍未能清楚說明監管制度。

廣告自動播片 港用家：愈強迫愈反感

香港文匯報訊（記者 陳敏婷、實習記者 林嘉敏） 本港市民周先生表示，發現愈來愈多手機應用程式的廣告自動播出影片，十分浪費數據，認為這是不好的宣傳手法，「愈強迫我看我愈反感」。

黎小姐亦認為手機應用程式的廣告煩厭，「如果彈出一兩個還可以忍，但如果太多太密，寧願刪掉該程式」。

張同學則指暫時未受相關廣告程式困擾，但得悉事件以後，下載手機應用程式時會更小心選擇，不下載來歷不明的應用程式，亦會先看清楚存取權限要求。