2012 年第三季之手機資安現況

根據卡巴斯基防毒公司的資料，在今年第三季所捕捉到手機的惡意軟體數量已經超過 9000 隻，比起今年第一季還要多出 3500 隻，顯現出在現今智慧型手機逐漸成為人手必備的時期，也開始被網路犯罪份子所盯上。

目前第三季手機的惡意軟體數量仍然是以 Android 平台為主流，所遭受感染的版本中以 2.3.6 的 Gingerbread 佔 28%為最多數，主因是現今在智慧型手機的持有率仍以 2.3.6 版本為大宗。第二名為佔 22%的 4.0.4 Ice Cream Sandwich 版本，原因是會更新成 4.0.4 的使用者通常具有使用手機上網的習慣，因此他們也容易在上網時會去瀏覽到惡意網站或是下載到惡意軟體。

手機惡意軟體的種類在第三季是以會寄送 SMS 簡訊的木馬程式為最常見，佔了目前總數量中了 57%，其中以 Opfake、Plangton 和 FakeInst 這三個惡意軟體家族佔居前三名。以下就簡單介紹這三種惡意軟體：

- Opfake – 是一隻會寄送 SMS 簡訊到高費率號碼的手機木馬程式，主要於一月份開始流行。Opfake 會將自身偽裝成 Opera 瀏覽器的手機版 App - Opera Mini 的安裝程式，來誘騙不知情的使用者去下載安裝。在七月份時，網路犯罪份子甚至也將下載網頁偽裝成跟官網的下載網頁一樣，以增加真實程度來進行欺騙。
- Plangton –主要會偷偷地收集你手機上的資訊，並且利用網路傳送給網路犯罪份子，網路犯罪份子也可以傳送指令給這隻惡意程式以進行下個動作，意味著 Plangton 若進行更新時，可以不需要經過使用者權限便可自行更新。Plangton 也會將你瀏覽器的首頁和書籤偷偷地進行更改。
- FakeInst –FakeInst 主要也跟 Opfake 一樣擁有寄送 SMS 簡訊的行為。為了不讓資訊安全人員了解到程式內部，FakeInst 會將自己的檔案利用 AES 加密演算法加密。

由於手機惡意程式本身並不能自行散佈，因此網路犯罪份子經常使用社交工程的手段吸引使用者來下載，其中又以在第三方網站所下載的程式最為危險，因此建議使用者不要從不信任的第三方網站下載程式。在安裝前，也應詳細閱讀程式的權限需求，因為檢查權限需求便可以知道一些惡意軟體所偽裝的正常 App 會出現不一致的權限要求，例如一個賽車遊戲會出現寄送三封簡訊至服務者的請求，一般來說這是不合理的。以及隨時檢查所安裝 App 的使用權限，以防止惡意軟體偷偷地寄送簡訊或傳送資料，這樣才能保障使用智慧型手機的安全。

◆ 參考來源：

[1]. http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_201

2

[2]. http://www.symantec.com/security_response/writeup.jsp?docid=2012-012709-2732-99

[3]. http://news.softpedia.com/news/Avast-Warns-About-FakeInst-and-Alternative-Android-Markets-269380.shtml

[4]. https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan%3AAndroidOS%2FPlankton.A