下載 Keepass 與 7-Zip 等知名軟體，小心誤闖山寨官網被植入廣告程式

研究人員 Ivan Kwiatkowski 發現駭客藉由仿造知名軟體官網，誘導使用者下載以散佈廣告程式，駭客相中的知名軟體包括 Keepass、7-Zip、Clonezilla 及 Greenshot 等等。

文/陳曉莉 | 2018-07-30 發表

一名安全研究人員暨惡意程式分析師 Ivan Kwiatkowski 上周揭露駭客仿冒了眾多知名開源軟體的官網，誘導使用者下載並安裝相關軟體，卻在軟體中植入了廣告程式來牟利。

Kwiatkowski 最早發現的是假冒為 Keepass 的 Keepass.fr。Keepass 為一開源的密碼管理程式，支援 Windows、macOS 與 Linux 等作業系統，它的官方網站為 Keepass.info，但駭客卻建立了 Keepass.fr，企圖魚目混珠。

Kwiatkowski 的發言引起了另一名安全研究人員 Lewis 的迴響，雙方你來我往地在 Twitter 上建立清單，顯示不只是 Keepass，受到駭客

青睞的知名軟體還有 7-Zip、Clonezilla、Greenshot 與 Audacity 等，有些同時提供了法國（.fr）與西班牙（.es）的仿冒網站，而且這些網站的申請人都是來自於同一個帳號。

例如除了假的 Keepass.fr 之外，駭客還建立了 Keepass.com；而壓縮程式 7-Zip 的官網為 7-zip.org，但駭客建立了 7zip.fr；而由台灣國網中心所開發的Clonezilla 硬碟克隆軟體官網應是clonezilla.org，駭客則為其打造了 clonezilla.es 及 clonezilla.fr；開源螢幕截圖軟體 Greenshot 的官網是 getgreenshot.org，網路上則有假冒的 greenshot.fr；開源的錄音與音訊編輯軟體 Audacity 的官網為 audacityteam.org，駭客亦建立了 audacity.es 與 audacity.fr。

其它遭到駭客利用的熱門軟體至少還包括 Celestia、Notepad2、Paintnet、Scribus、Azureus、Unetbootin、Inkscape、Handbrake、Gparted、Stellarium、Gimp 與 Thunderbird。

資安專家則建議使用者要下載自由或開源軟體前，得先確定官網位址，就算自以為是從官網下載，也最好經由防毒軟體進行掃描。

資料來源：iThome