

惡意軟體假冒「 Windows Update 」更新視窗竊個資！小心電腦遭駭入侵

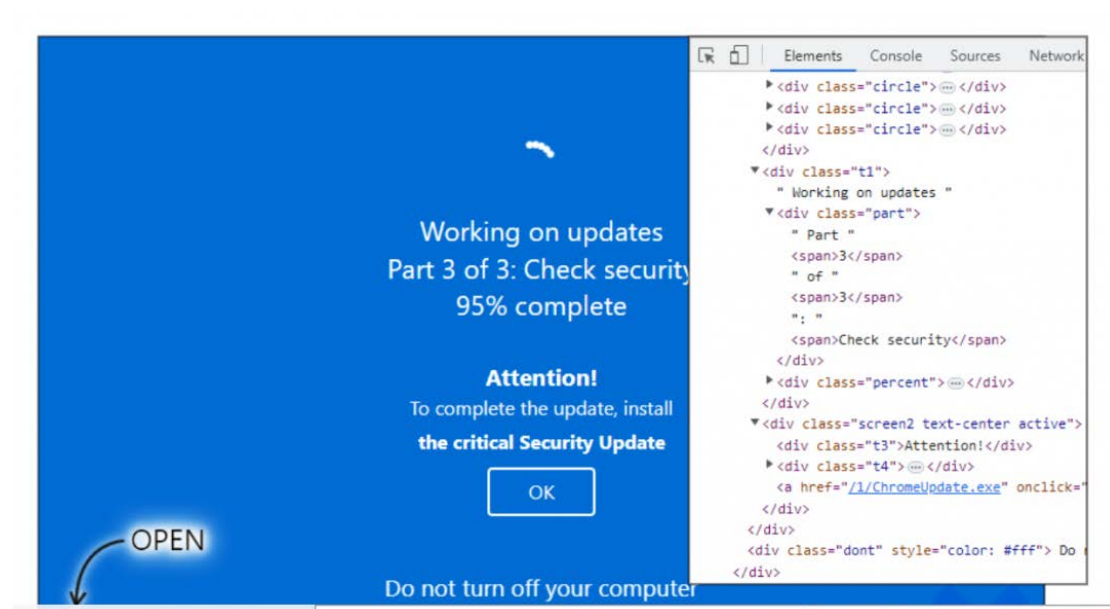


(圖 / 路透)

近期使用瀏覽器上網逛網頁時，要是電腦螢幕突然跳出視窗，且畫面顯示為「Windows Update」更新內容等相關字眼，可要多加留意！千萬別依照畫面指示按下 OK 按鈕，更不要執行安裝或下載任何軟體，以免誤入駭客發動惡意攻擊活動的陷阱，導致電腦恐不慎感染會暗中擅自竊取裝置個資的 Aurora 惡意軟體。

資安業者 [Malwarebytes](#) 旗下研究人員指出，近期於網路上偵測到有不肖駭客份子正利用假冒微軟「Windows Update」更新

內容的視窗形式作為誘餌，把彈出式視窗的內容包裝成以全螢幕顯示，偽裝度極逼真的微軟 Windows 系統更新內容畫面，不但會有執行更新的轉圈圈圖示，顯示正在更新進度百分比的數據、與不要關閉電腦等文字描述，且當更新進度的數字為顯示百分百之後，還會聲稱，需按下「OK」按鈕，以完成更新。然而，一旦點擊「OK」按鈕之後，接著就會自動下載一個被命名為「ChromeUpdate.exe」的執行檔。



假冒微軟 Windows Update 更新內容的彈出式視窗，暗藏竊取個資惡意間諜軟體。（圖翻攝 Malwarebytes 部落格）

雖然文件檔案名稱顯示為「ChromeUpdate.exe」，但實際上只是用來騙過防毒軟體偵測惡意軟體所用的假名稱障眼法，實際上本質則是具備有可從遠端獲取電腦系統憑證，得以入侵裝置竊取個資的 Aurora 惡意間諜軟體。

有關這波假冒微軟「Windows Update」更新視窗的惡意攻擊活動，Malwarebytes 進一步分析表示，駭客採取的手法是藉由高流量的國外成人色情網站作為散播惡意軟體的主要途徑，並把彈出式廣告內容，巧妙包裝成全螢幕覆蓋、假冒為微軟「Windows Update」更新內容的樣式設計，讓不知情的受害者誤以為是電腦系統自動跳出的更新畫面。

建議 PC 電腦用戶需安裝任何 Windows 更新檔時，務必從微軟官方的更新目錄網站上，查找所需的檔案並於微軟官網下載。若瀏覽器突然跳出可疑的更新視窗時，不要執行任何點擊的動作，並關閉瀏覽器。另，也可安裝可偵測惡意廣告活動的防毒軟體，以保護電腦裝置避免遭駭入侵的資安威脅風險。

文章摘自：自由電子報