自由時報

中國變種木馬 綁架桌面捷徑

連結到中國網站百度或淘寶等

〔記者王珮華／台北報導〕資安業者近期觀察新一波木馬程式攻擊，發現名為Troj_malware.vtg的木馬，會竄改使用者桌面捷徑，只要使用者點下這些捷徑，就會連到中國知名網站，如百度、淘寶等，推測木馬的作者可能是對岸駭客。資安業者建議，透過修改登錄檔，可解決桌面捷徑被綁架的問題。

趨勢科技表示，最近發現一隻名為Troj_malware.vtg的變種木馬程式，一旦網友瀏覽帶有此木馬程式的網頁，會跳出視窗詢問是否要執行某些程式，不論網友接受與否，此惡意程式將自動執行，讓使用者的檔案捷徑失效，點選任何捷徑都會被連到某些中國知名網站如百度、淘寶等，捷徑形同綁架。

趨勢科技資深技術顧問簡勝財指出，該木馬目前在中國與台灣都有發現，由於木馬程式可能被駭客植入任何網站，因此

無法得知瀏覽哪些網站會中招。不過，從木馬執行時，會跳出簡體中文視窗來看，這隻木馬作者有很大機會是對岸人士，也推測網友瀏覽中國網站時，遭感染的機會比較大，請網友特別小心。

簡勝財說，目前觀察到被感染的檔案捷徑將無法自桌面直接修復，須經手動於系統中修復，造成網友使用電腦的不便，至於遭感染的電腦是否會有其他風險，目前還沒發現，依照駭客行為模式，可能是在測試某些更具威脅性的惡意工具。簡勝財提醒，由於此隻木馬程式變種速度快且多，網友最好勿輕易瀏覽不明網站。

趨勢科技也提供修復方式，網友可在「附屬應用程式」中找到「執行」，輸入「regedit」，按下「編輯-->尋找」，輸入被綁架前往的目的網址，找到左方相對應的 CLSID 值；之後，再「編輯-->尋找」，輸入 CLSID 值，將搜尋到的登錄值全數刪除，即大功告成。

連結網址：

http://tw.news.yahoo.com/article/url/d/a/100729/78/2a3og.html