◎資訊安全宣導

—小心！駭客以假憑證過期通知散佈惡意程式—

惡意軟體假冒合法軟體騙取用戶上鉤時有所聞，像是謊稱成新版瀏覽器或新版 Adobe Flash Player，讓造訪被駭網站的用戶不疑有他下載。安全廠商卡巴斯基發現又有新招，有後門及木馬程式假冒網站憑證過期的通知訊息，誘使訪客點擊下載。

網頁 SSL/TLS 憑證是由憑證機構（CA）簽發，可驗證網站身份不是釣魚網站，以及在用戶瀏覽器和網頁伺服器之間建立加密連線以確保資訊的隱私性。因此 SSL/TLS 憑證是安全上網的關鍵，而啟用 SSL/TLS 憑證的網站，就會顯示 HTTPS 為開頭的網址，Chrome、Firefox、Safari、Edge 等瀏覽器，都已預設不支援 HTTP 的網站。

但最近卡巴斯基發現有駭客濫用此類憑證散佈後門程式。用戶連進被駭網站後，網頁顯示「安全憑證過期」的警告訊息，告知需要更新網頁憑證才能繼續瀏覽，並以按鍵引導用戶下載。卡巴斯基偵測，此類攻擊最早出現於今年 1 月 16 日，現今已出現於多種主題網站上，從動物園到汽車零件經銷商等。

卡巴斯基指出，Buerak 進入 Windows 電腦後會執行程式、修改程式行程、竊取資料、還會經由機碼潛伏在電腦中。而 Mokes 則是 macOS/Windows 後門程式，可執行程式碼、竊取資料或影音檔案，並偷偷進行截圖。

SSL 憑證最近也成為資安關注焦點。免費憑證發行機構 Let's Encrypt 發現，它所使用的憑證機構軟體有臭蟲，導致誤發憑證，得撤銷 3 百萬個 TLS/SSL 憑證。另外，蘋果、Mozilla 和 Google 也認為憑證效期太長不安全，因而計畫將縮短支援的 SSL/TLS 憑證效期，這可能迫使網站更頻繁更新憑證。

【文章擷取-iThome 新聞】

臺中榮民總醫院提醒你!也關心你!