Petya 勒贖軟體來襲，專家教你暫時自保方法

Petya 感染被害者的電腦後會先檢查磁碟內是否有檔名為 perfc.dll 的檔案，如果發現同名檔案就不會進行加密，安全專家教導使用者可先在電腦內建立一個同名檔案，暫時躲過加密。

文/林妍溱 | 2017-06-28 發表

WannaCry 才在上個月引發全球災難，周二又有一隻名為 Petya 的勒贖軟體再度侵襲全球 Windows PC。有安全專家率先提出免於被害的暫時性方法。

如同 WannaCry，Petya 也是利用美國國安局(NSA)被「影子駭客」外洩的攻擊工具 EternalBlue，用以入侵 Windows PC。災情最重地區為歐洲；烏克蘭的中央銀行、國營電信公司、地鐵及首都基輔機場、車諾比爾核電廠、超市 POS、俄羅斯國營石油公司皆被植入 Petya，另外美國知名藥廠默克(Merck)、法律事務所 DLA Piper 及多家醫院也遭到感染。

和一般勒贖軟體相同，感染後，它會加密檔案，並跳出訊息，要求受害者支付相當 300 美元的比特幣到其所附的區塊鏈網址。

一開始研究人員以為它是以前一個叫 Petya 的惡意程式新變種，不過後來發現它其實是不同程式，只是有一部份程式碼取自 Petya。因此後來有人為之起了 NotPetya、Petna 或 SortaPetya。

一名為 Amit Serper 的安全專家發現一個方法可保用戶暫時不被加密勒索。NotPetya 會先搜尋受害電腦的本機檔案，如果發現磁碟內已經有同名檔案，就不會進行加密。Serper 指出，這隻惡意程式的檔名為 perfc.dll，只要受害者在 PC 的 c:\Windows 檔案夾中建立名為 perfc 的無副檔名檔案，設為唯讀，就可以防止這隻惡意程式執行。而許多人試用後也證明可行。

微軟在 WannaCry 攻擊爆發時已經針對 Windows 新舊版發佈修補程式，包括 XP。因此補好的 Windows PC 應該不用擔心。然而從 NotPetya 再次席捲各國，顯見 Windows 更新的情況還是未儘理想。

資料來源：iThome