預防 Petya 勒索病毒攻擊的方法

一、前言

繼 106 年 5 月中旬 WannaCry 勒索病毒事件後，近日在全球各地陸續爆發新型勒索病毒 Petya，尤其以歐洲最為嚴重，該病毒非之前舊型 Petya 病毒，而其攻擊行為比 WannaCry 病毒更勝一籌，駭客除了使用 SMBv1 漏動外，也會利用 Windows 的遠端指令功能 PsExec 或是 WMIC（Windows Management Instrumentation）來執行命令，包括傳染至其他電腦。為避免感染此病毒，建議使用者盡快做好防範措施。

二、病毒資訊

NO	項目	內容
1	病毒名稱	Petya（又名 NotPetya、Petwrap 或稱 Petya.2017）
2	微軟編號	MS17-010
3	CVE 編號	CVE-2017-0199
4	病毒特徵	Petya 勒索病毒是經由 Microsoft 官方提供的 PsExec 遠端執行工具或是 WMIC 來進入電腦系統，也會搭配 EternalBlue 這個漏洞攻擊套件來攻擊 SMB v1 漏洞。一旦 Petya 進入電腦會利用程式 rundll32.exe 來執行其程式碼，其檔案加密程式碼是放在 Windows 資料夾底下一個名為「perfc.dat 」的檔案內，接著會自動建立排程，設定電腦於 1 小時內重新開機來啟動加密機制，也會利用這一小時掃描電腦所在的區域網路。另外，Petya 鎖定加密的檔案大多是企業常使用的檔案類型，甚至也會直接攻擊文件系統。特別的是，遭 Petya 加密的檔案，不會變更其副檔名。在電腦重新開機後，會修改受害電腦之作業系統開機磁區(MBR)，並且加密硬碟的檔案配置表(MFT)。 當加密檔案的程序完成後，使用者會看到要求贖金的畫面，要求受害者支付相當於 300 美元（約合新台幣 9,173 元）的比特幣到攻擊者所提供的單一錢包，取得單一識別碼再寄一封電子郵件到某個 @posteo.net 的信箱告知。付款後可透過該信箱與攻擊者通信以換取解密金鑰，但目前該信箱已被電子郵件服務商停用，這表示受害者已無法與攻擊者通信要求解密，又由於 Petya 病毒對受害者的電腦所建立的個別安裝 ID 碼是隨機產生的，該 ID 碼的主要用途是提供駭客辨認受害者，以便駭客提供解密金鑰給已付贖金的受害者，可是當 ID 碼是隨機產生意謂著不可能再解密檔案，即使受害者付了贖金也救不回資料。
5	受影響 作業系統	Windows XP Windows Vista

NO	項目	內容
		Windows 7 Windows 8.1 Windows RT 8.1 Windows 10 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016

三、建議措施

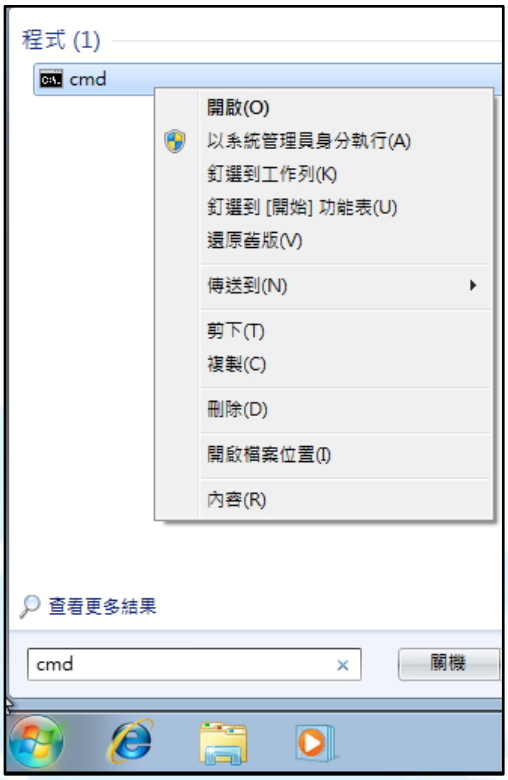
1. 設定 Windows 密碼與加強密碼強度

為避免攻擊者破解使用者密碼，建議使用者務必設定登入 Windows 的密碼，並且加強密碼強度，建議設定含英文及數字組合之 8 位以上的密碼，並定期變更密碼。以 Windows7 系統為例，使用者可至「控制台>使用者帳戶和家庭安全>使用者帳戶>」內變更密碼。

2. 建立預防 Petya 的 Kill - Switch 檔案

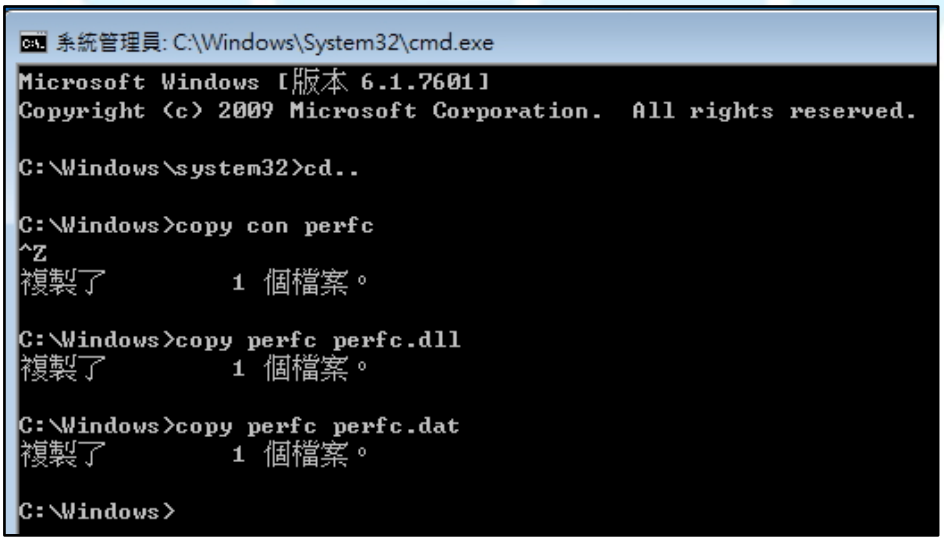
為了預防感染 Petya 病毒，使用者可自行於 C:\Windows 目錄下建立病毒加密時會使用的檔案，來中斷病毒程式的執行。建立檔案的方式以 Windows 7 系統為例，說明如下:

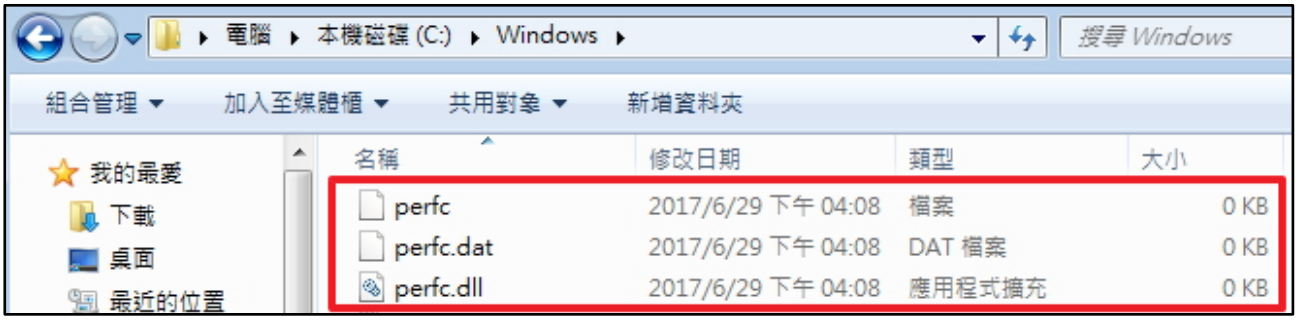
(1)以系統管理員身分執行「命令提示字元」。



(2)輸入以下指令，在 C:\Windows 資料夾中建立 perfc、perfc.dll 與 perfc.dat 等三個檔案。

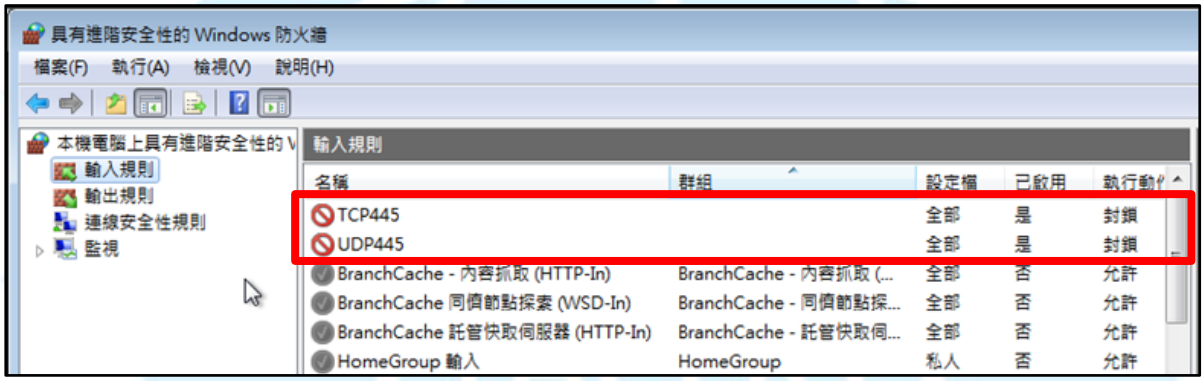
No.	指令內容	說明
1	cd..(按 Enter)	至 C:\Windows 目錄下
2	copy con perfc(按 Enter)	複製產生一個空白內容的 perfc 檔案
3	(按 Ctrl+Z)	中斷
4	(按 Enter)	完成複製
5	copy perfc perfc.dll	複製產生一個 perfc.dll 檔案
6	copy perfc perfc.dat	複製產生一個 perfc.dat 檔案





3. **關閉 Windows 系統的 445 連接埠。**

為預防 Petya 病毒透過 445port 滲入，建議使用 Windows 系統內新增防火牆輸入規則的方式，封鎖 445 連接埠的連線。以 Windows7 系統為例，使用者可至「控制台」>「系統及安全性」>「Windows 防火牆」>「進階設定」內，新增兩條輸入規則鎖住 445 連接埠。



4. **定期使用隨身碟、外接硬碟或者雲端空間備份重要資料。**

當電腦感染到 Petya 病毒時，尚無任何還原程式可將被加密的檔案解密，因此建議使用者定期進行資料備份。

5. **使用 Windows Update 自動更新或手動更新微軟的 Windows 的 SMBv1 漏洞修補程式(漏洞編號 MS17-010)與 Office 應用程式弱點修補程式(漏洞編號 CVE-2017-0199)**

可至微軟官方網站下載修補程式進行更新，參考網址如下。

(1)MS17-010:

https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx

(2)CVE-2017-0199:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

6. **確認防毒軟體已更新至最新版本病毒碼與偵測程式碼，並定期執行電腦掃毒作業。**

7. **因病毒執行加密時會建立排程，讓系統自動重新開機，建議使用者發現系統無預警自動重新開機時，應即刻關閉電腦電源，以避免進一步的加密行為。**

參考資料:

1. Petya Ransomware Spreading Rapidly Worldwide, Just Like WannaCry
http://thehackernews.com/2017/06/petya-ransomware-attack.html
2. Analyzing the Fileless, Code-injecting SOREBRECT Ransomware
https://blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/
3. Petya 病毒全球爆發中 ！比 WannaCry 強 電腦更新過也中招 ：Windows 香港受害者上升中
https://unwire.hk/2017/06/28/petya/top-news/
4. 《勒索病毒警訊!》Petya 大規模爆發中,三步驟防範感染
https://blog.trendmicro.com.tw/?p=50559