TCP 445 通訊埠的關閉方式 (簡國璋 撰稿)

近日,新的一波變種勒索病毒 Petya 正四處肆虐中,相較於五月間造成全球恐慌的 WannaCry 勒索病毒, Petya 的散播管道主要有兩種:

- 同樣是利用微軟的安全弱點: MS17-0106 Etetnalblue 來針對使用者進行攻擊,不同於 WannaCry 的地方, Petya 入侵電腦後,會修改電腦硬碟中的主要開機磁區(Master Boot Record, MBR)的設定,而且建立電腦 排程於一小時內重新開機,開機時會於電腦螢幕跳出勒索訊息視窗,讓使用者無法進行任何操作。
- 2. 駭客會利用微軟官方的 PsExec 遠端執行工具,以「進階持續性滲透攻擊」(Advanced Persistent Threat, APT) 的手法進行入侵,一旦入侵成功,將可以潛伏於內部網路中並感染控制內部重要伺服器,進一步發動勒 索病毒攻擊。

對此,本中心建議本校同仁應採取以下防範措施來避免感染:

1. 套用安全性弱點 MS17-010 EternalBlue (<u>https://technet.microsoft.com/zh-tw/library/security/ms17-</u>010.aspx)修補更新。

2.停用 TCP 連接埠 445。

停用 TCP 連接埠 445 的步驟如下:

步驟1、開啟「控制台」,選擇「系統及安全性」,如下圖所示。



步驟 2、選擇「Windows 防火牆」,如下圖所示。

	全性▶	 世界 授募控制台
檔案(E) 編輯(E) 檢視(V) 工具(I)	說明(出)	
控制台首頁 ● 系统及安全性	P	行動作業中心 檢閱電腦的狀態和解決問題 🌍 變更使用者帳戶控制設定 疑難排解常見電腦問題
網路和網際網路 硬體和音效		整實經過原到範疇的時間 Windows 防火牆 檢查防火臟狀態 · 允許裡式通過 Windows 防火牆
程式集 使用者帳戶 外觀及個人化		糸統 檢視 RAM 大小及處理器速度 │ 檢查 Windows 體驗指數 │ 發 允許遠端存取 │ 查看此電腦的名稱 │ 發 裝置管理員
時鐘、語言和區域 輕鬆存取	2	Windows Update 開啟或關閉自動更新 檢查更新 檢視已安裝的更新
	1	電源選項 唤醒電腦時必須輸入密碼 變更電源按鈕行為 變更電腦睡眠的時間
	R.	備份與還原 備份電腦 │ 從備份邊原檔案
	2	Windows Anytime Upgrade 取得新版 Windows 7 的其他功能
	(îi	糸統管理工具 釋放磁碟空間 重組您的硬碟 ♥ 建立及格式化硬碟磁碟分割 ♥ 檢視事件記錄檔 ♥ 排程工作
	£	Flash Player

步驟3、選擇「進階設定」,如下圖所示。

●●●●● ▶ 控制台 ▶ 糸統及安	全性 ▶ Windows 防火牆	- □ X
檔案(E) 編輯(E) 檢視(V) 工具(I)	說明(出))
控制台首頁 允許程式或功能通過 Windows 防火牆 變 變更通知設定	使用 Windows 防火牆來協助保護約 Windows 防火牆有助於防止駭客及惡意軟體認 防火牆如何協助保護我的電腦?	② ② 您的電腦 ◎ 過網際網路或網路存取您的電腦。
● ● ● ● ● ● ● ● ● ● ● ● ● ●	什麼是網路位置? 初域網路(<u>M</u>) 連結到網域之工作地點的網路	已連線 🔊
先此期11分1月9日30日1月1日	Windows 防火牆狀態: 連入連線: 使用中的網域網路:	開啟 封鎖對於不在允許的程式清單中之程式的所有連入 連線 i takming.edu.tw
	 通知広思: ② 家用或工作場所(私人)網路 ◎ 公用網路(P) 	 A (Q) 未連線 ◆ 未連線 ◆
請參閱 行動作業中心 網路和共用中心		

步驟 4、選擇「輸入規則」、「新增規則(N)...」,如下圖所示。



步驟 5、選擇「連接埠」後,點選「通訊協定及連接埠」,如下圖所示。

一新用朝八號則稱靈 規則類型 選取要建立的防火牆規則類型	
# 相則類型 通訊協定及連接埠 ● 執行動作 ● 設定檔 ● 名稱	#要理立 確 類 型 的 規 即 。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・
	<上一步(B) 下一步(N) > 取消

步驟 6、點選「TCP」和「特定本機連接埠」, 輸入 445, 按下「下一步」, 如下圖所示。

新增輸入規則精整	
通訊協定及連接埠	
指定套用這個規則的通訊協定	與連接埠。
步驟:	此規則會套用至 TCP 或 UDP?
• 規則類型	● TCP(T)
• 通訊協定及連接埠	() UDP(U)
• 執行動作	
• 設定檔	這個規則套用至所有本機連接埠或特定本機連接埠?
• 名稱	◎ 所有本機連接埠(A)
	◎ 特定本機建接埠(2): 範例: 80, 443, 5000-5010
	深入了解通訊協定及連接埠
	<上一步(B) 下一步(D) > 取消

步驟7、點選「封鎖連線」,按下「下一步」,如下圖所示。

💣 新增輸入規則精靈	
執行動作 指定要在連線符合規則中指定	的條件時採取的動作。
步驟: 規則類型 通訊協定及連接埠 執行動作 	當連線符合指定的條件時,應採取哪些動作? ⑦ 允許連線(A) 這包含使用 IPsec 保護的連線,以及未使用 IPsec 保護的連線。 ⑧ 僅允許安全連線(C) 這口句全尸使用 IPsec 驗證的連線。會使用 [連線安全性報目]] 節點中的 IPsec 內茲和
 設定檔 名稱 	○ 封鎖連線(K)
	<u>深入了解動作</u> < <u>∠</u> 上一步(B) 下一步(Δ)> 取消

步驟8、將「網域」、「私人」與「公用」都勾選,按下「下一步」,如下圖所示。

💣 新增輸入規則精靈	And a second of the second sec	X
設定檔		
相定安全而此规则的改定语。		
步驟:	何時會套用此規則?	
• 規則類型		
• 通訊協定及連接埠	✓ 網域(D) 営奮膨連線至其公司領域時套用。	
執行動作	▼ 私人(P)	
1 設定檔	當電腦連線至私人網路位置時套用・	
* 名稱	✓ 公用(U) 當電腦連線至公用網路位置時套用。	
	深入了解設定檔	
	(<上一步(B)) 下一步(N) > 取消	

步驟9、輸入足以辨識的名稱,按下「完成」,如下圖所示。

Para Bizentalijinjezii · Agningzii · Manakazojetysia · Mofishine · Bizetali · Agni	💣 新增輸入規則精靈			
少認: · 規則模型: · 通訊協定及連接埠 · 放行動作 · 設定檔 · 名稱	名稱 指定此規則的名稱與描述。			
 規則類型 通訊協定及連接傘 執行動作 設定檔 名稱 	步驟:			
	 規則類型 通訊協定及連接準 執行動作 設定檔 名稱 	名稱(L): WannaCry_445_Block 描述 (可省略)(D):		

步驟 10、可以看到新增了一條規則,若是不再需要,隨時可將其刪除,如下圖所示。

當案(E) 執行(A) 檢	視(⊻) 說明(丑)								
Þ 🤿 📶 🔂 🚺									
▶ 本機電腦上具有進降	書 輸入規則						Į	协作	
💶 輸入規則	名稱	群組	•	設定檔	已啟用	執行動作	~	輸入相則	
🗳 輸出規則	WannaCry 445 Block			全部	是	封鎖		朝八八元只」	<u>. 8</u> 6
🎝 連線安全性規則	360 Total Security			網域	是	允許		◙ 新增規	
■ 監視	360 Total Security			網域	是	允許		☞ 依設定	•
	@ 360 Total Security			網域	是	允許		7 仿野能	κ.
	@ 360 Total Security			網域	是	允許			
	Ask Toolbar Notifier			網域	是	允許		☞ 依群組	
	Ask Toolbar Notifier			網域	是	允許		檢視	•
	BlueSoleilCS			公用	是	允許	Ē	手立ちあり	
	@ BlueSoleilCS			公用	是	允許	1	g 里利登	
	ØBonjour 服務			網域	是	允許	1	▲ 匯出清	
	ØBonjour 服務			網域	是	允許		2 說明	
	Boson NetSim			網域	是	允許		100.43	_
	Boson NetSim			網域	是	允許	1	WannaCry	
	@dropbox.exe			網域	是	允許		● 停田規	
	Sdropbox.exe			公用	是	封鎖	-		
	Sdropbox.exe			公用	是	封鎖	•	》 勇下	
	@dropbox.exe			網域	是	允許	E	複製	
	Ødude			網域	是	允許			
	Ødude			網域	是	允許	1		
	⊘ hfs			網域	是	封鎖		内容	
	O hfs			網域	是	封鎖	1	? 說明	_

【一般宣導】

- 1. 敬請尊重智慧財產權,有關校園網路使用規範、智慧財產權之宣導及注意事項,請多予關注,相關網址 如下:<u>http://www.takming.edu.tw/cc/</u>。檢舉信箱:<u>abuse@takming.edu.tw</u> 或 <u>netcc@takming.edu.tw</u>。
- 2. 請勿安裝來路不明之非法軟體,以免觸法。
- 3. 查閱相關電腦技術資料,網址: <u>http://www.takming.edu.tw/cc/resources/document.htm</u>
- 4. ODF 園地: <u>http://www.takming.edu.tw/cc/resources/odf.htm</u>