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：

1. 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。

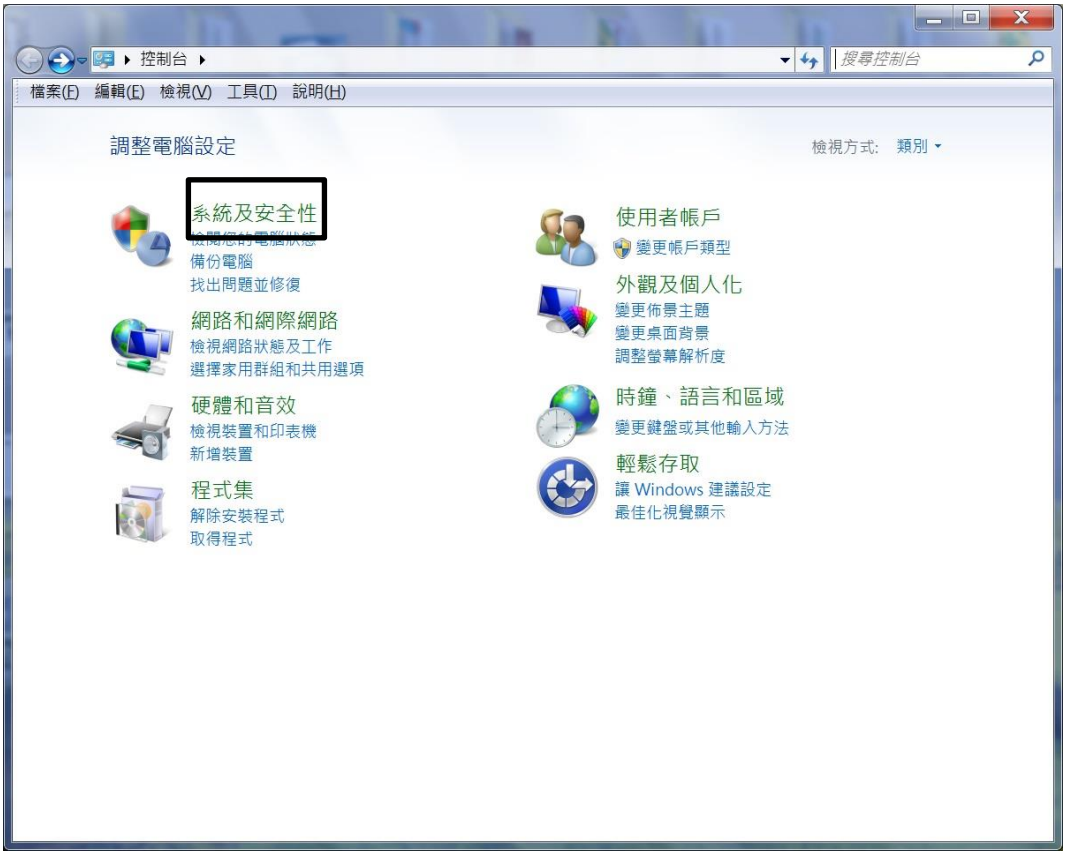
對此，本中心建議本校同仁應採取以下防範措施來避免感染：

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

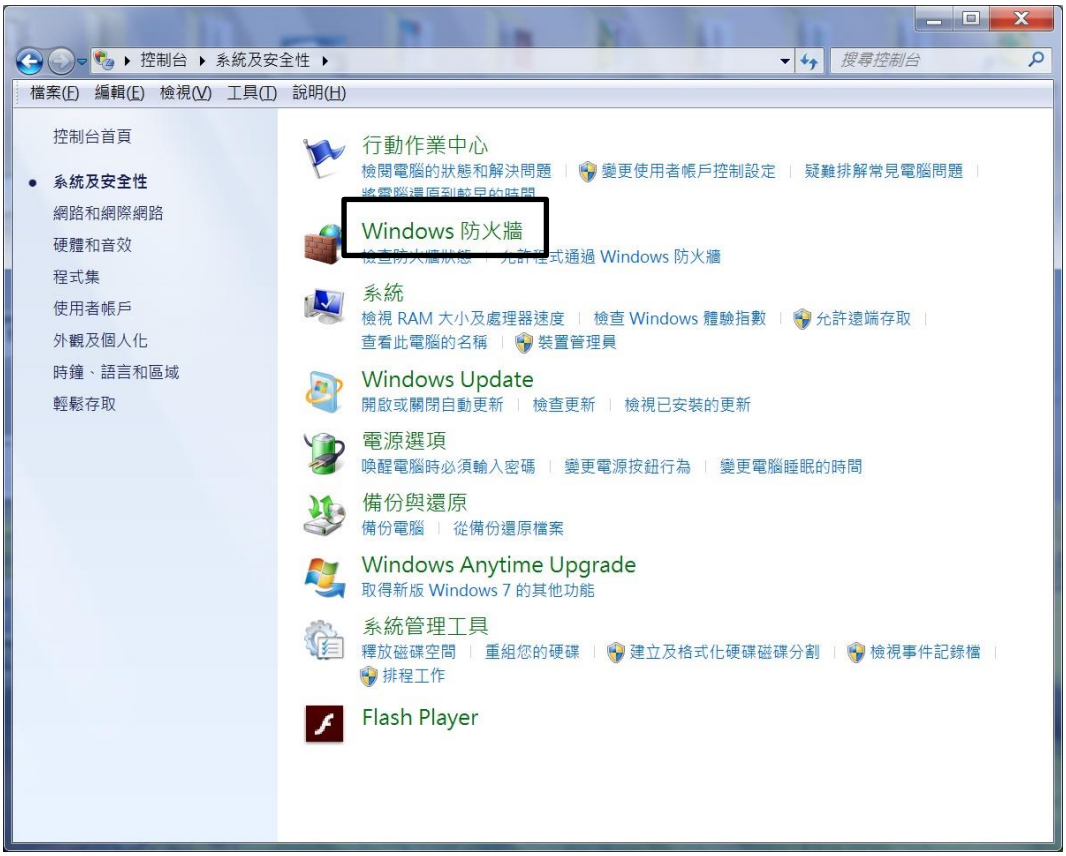
2.停用 TCP 連接埠 445。

停用 TCP 連接埠 445 的步驟如下：

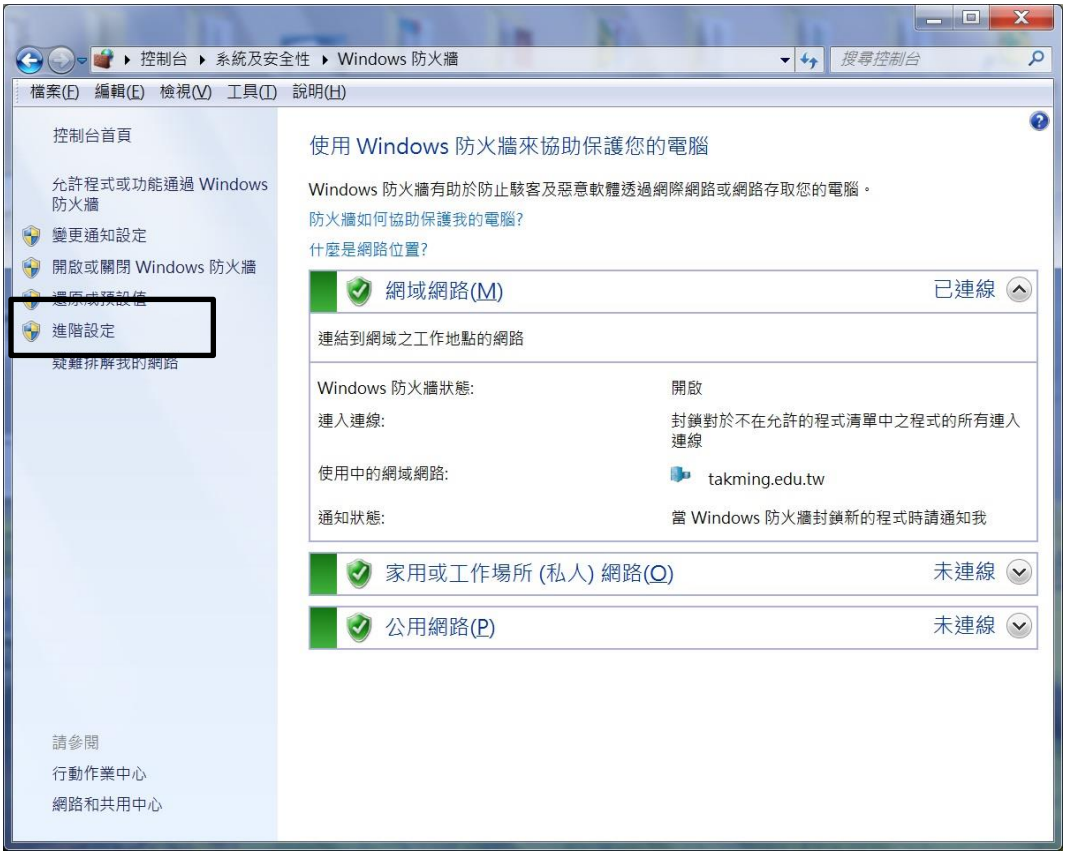
步驟 1、開啟「控制台」，選擇「系統及安全性」，如下圖所示。



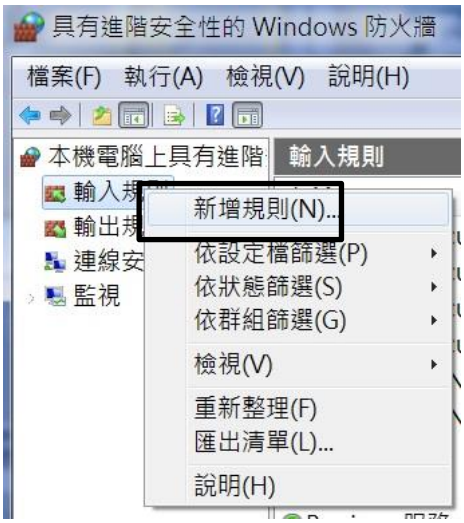
步驟 2、選擇「Windows 防火牆」，如下圖所示。



步驟 3、選擇「進階設定」，如下圖所示。

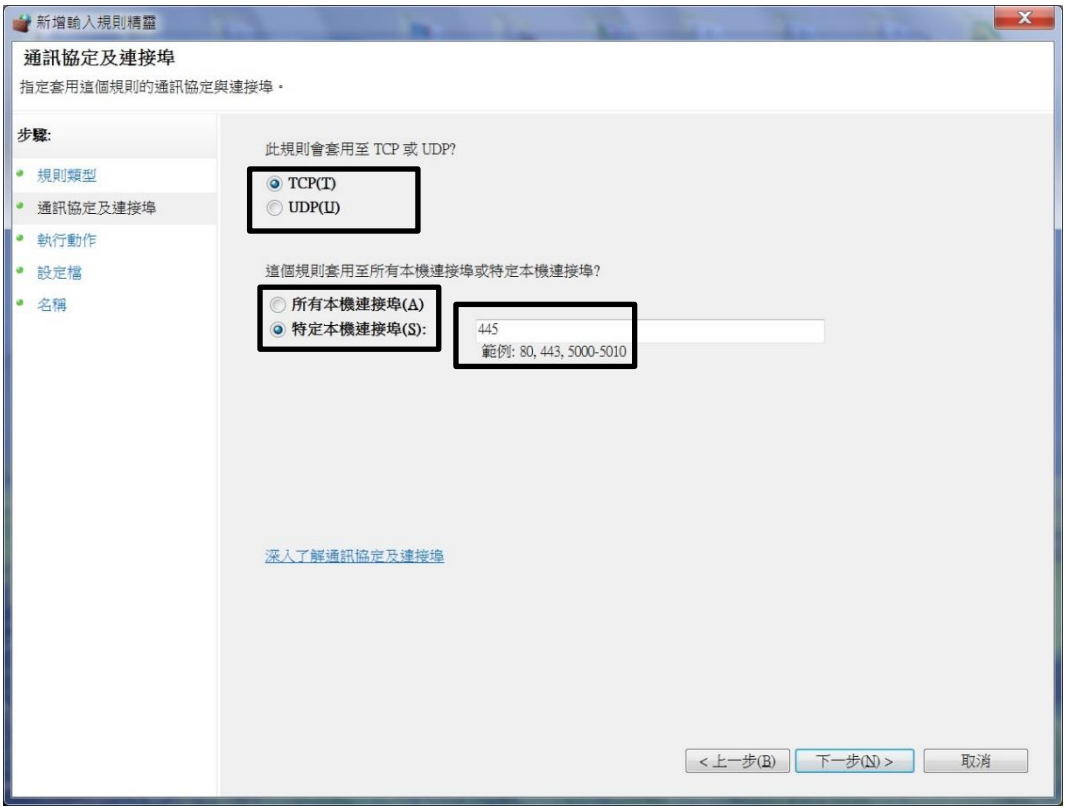


步驟 4、選擇「輸入規則」、「新增規則(N)...」，如下圖所示。

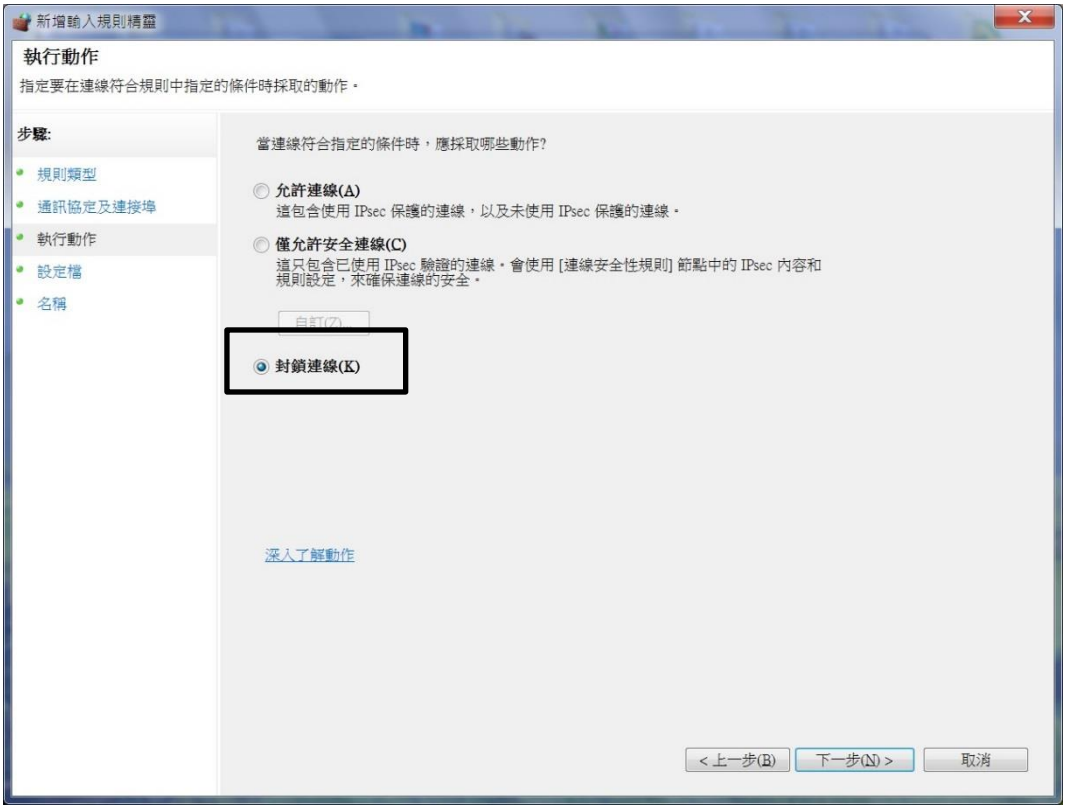


步驟 5、選擇「連接埠」後，點選「通訊協定及連接埠」，如下圖所示。

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。

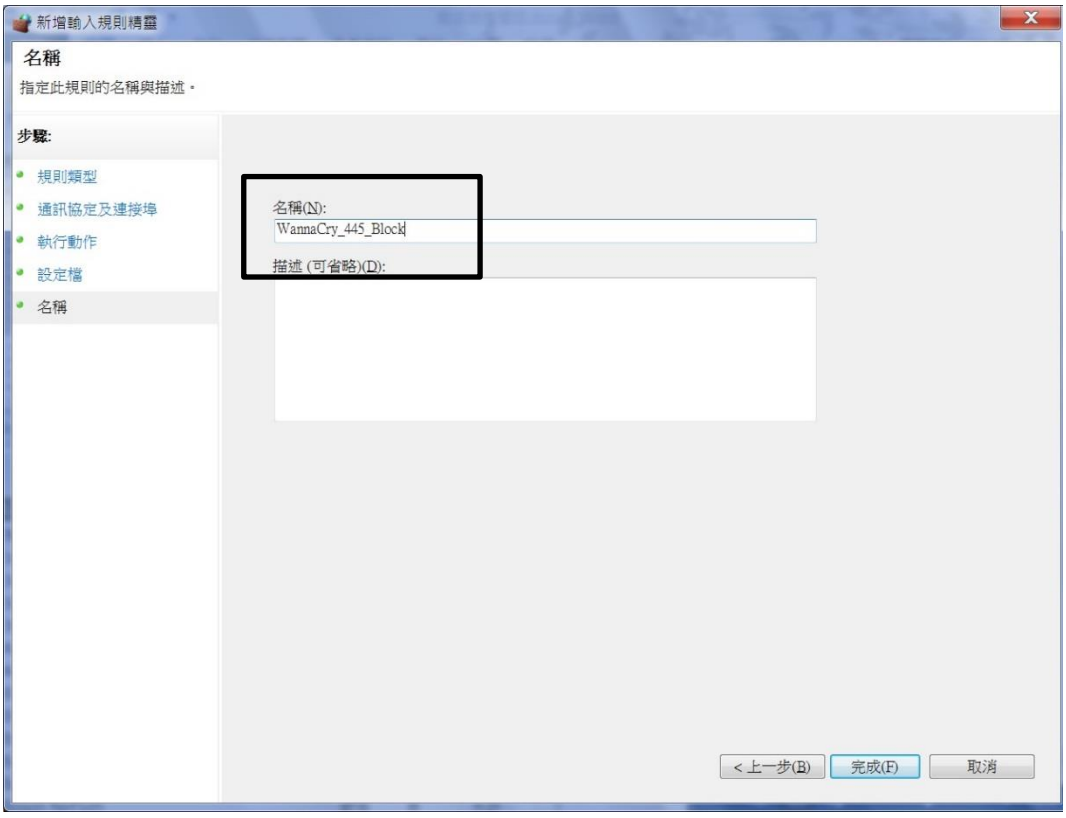


步驟 7、點選「封鎖連線」，按下「下一步」，如下圖所示。

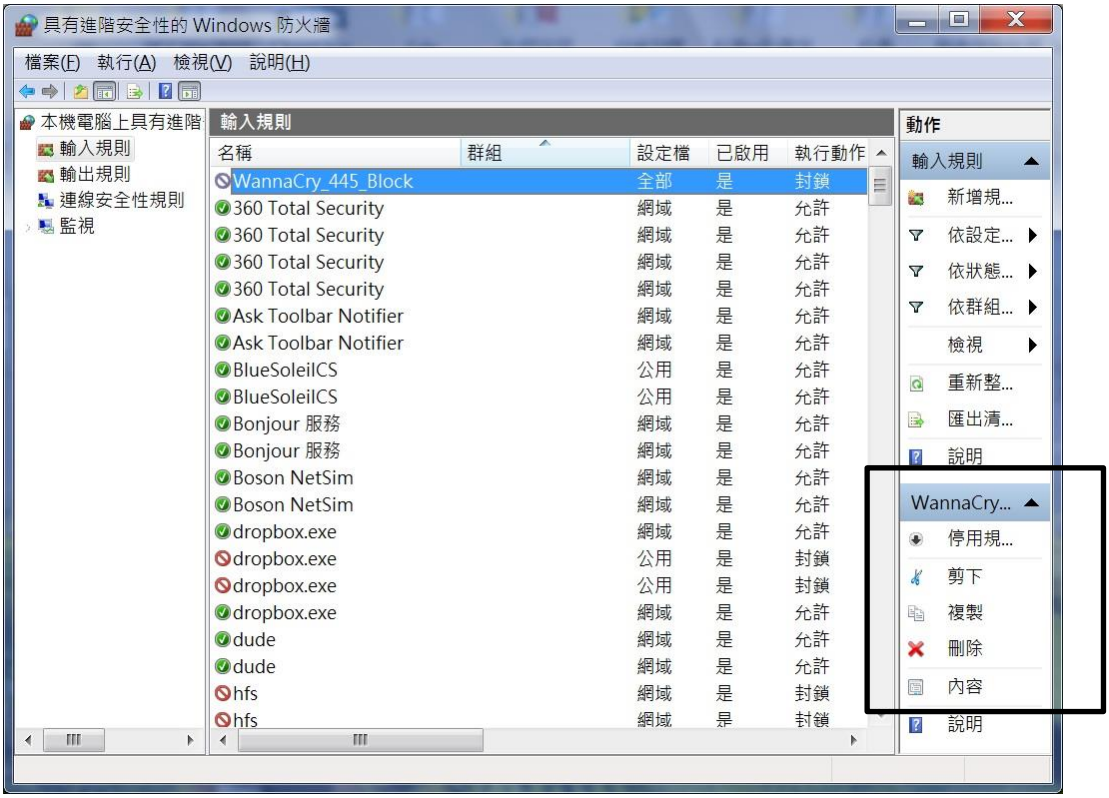


步驟 8、將「網域」、「私人」與「公用」都勾選，按下「下一步」，如下圖所示。

步驟 9、輸入足以辨識的名稱，按下「完成」，如下圖所示。



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。



【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：http://www.takming.edu.tw/cc/。檢舉信箱：abuse@takming.edu.tw 或 netcc@takming.edu.tw 。
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：http://www.takming.edu.tw/cc/resources/document.htm
4. ODF 園地：http://www.takming.edu.tw/cc/resources/odf.htm