臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

讓人想哭 WannaCry 勒索病毒

臺灣大學計資中心網路組
北區學術資訊安全維運中心

摘要

106 年 5 月 13 日是個看似如常的周末，殊不知網路上已掀起軒然大波，甚麼?不用開啟惡意檔案或點擊惡意連結也會中獎!一個名為「想哭 WannaCry」的勒索病毒，正在肆虐全球。

據統計，此事件大約於 5 月 10 日開始頻繁攻擊，而北區 ASOC 中心於 5 月 9 日偵測到此漏洞被利用的資安事件，並向對外攻擊的學校開立資安單，向遭受攻擊的學校發出告警通知。但勒索病毒的感染與傳播速度非常快速，短短數日內，包含台灣在內至少有 74 個國家遭受攻擊。

5 月 15 日周一上班日，統計至少 150 國逾 20 萬部電腦中毒。根據卡巴斯基實驗室的資料指出，台灣的想哭災情也進入了前四名，如圖 1 所示。

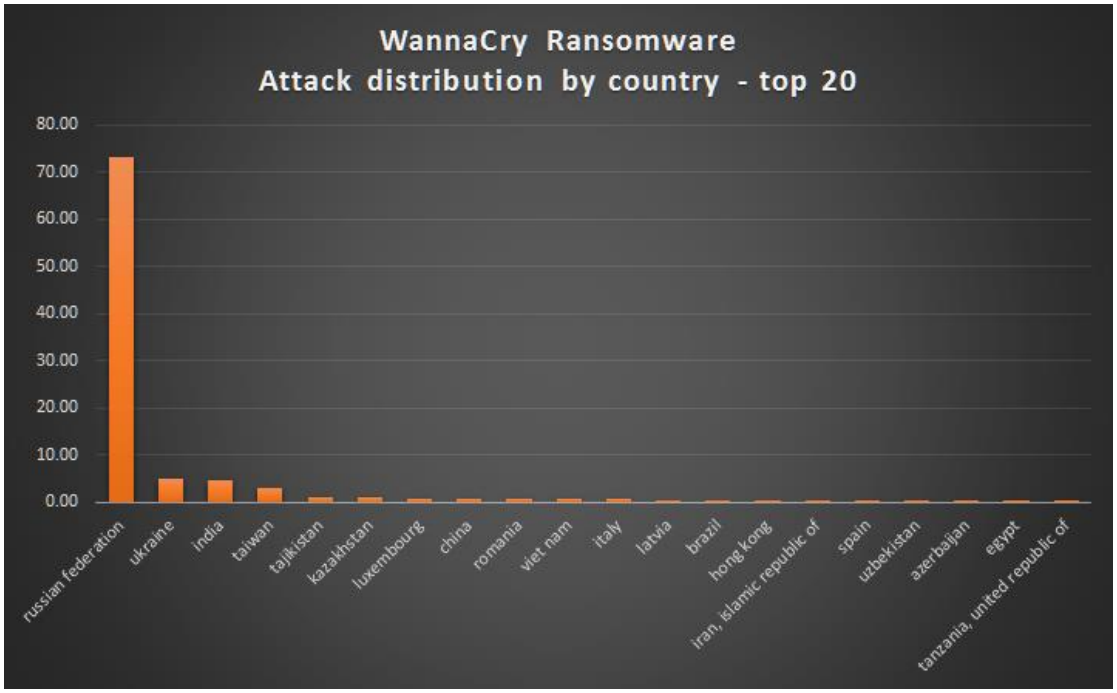


圖 1.　(圖片來源轉載自 https://goo.gl/pQQXV3)

圖 2 為全球各國遭受勒索病毒攻擊的分布情形。

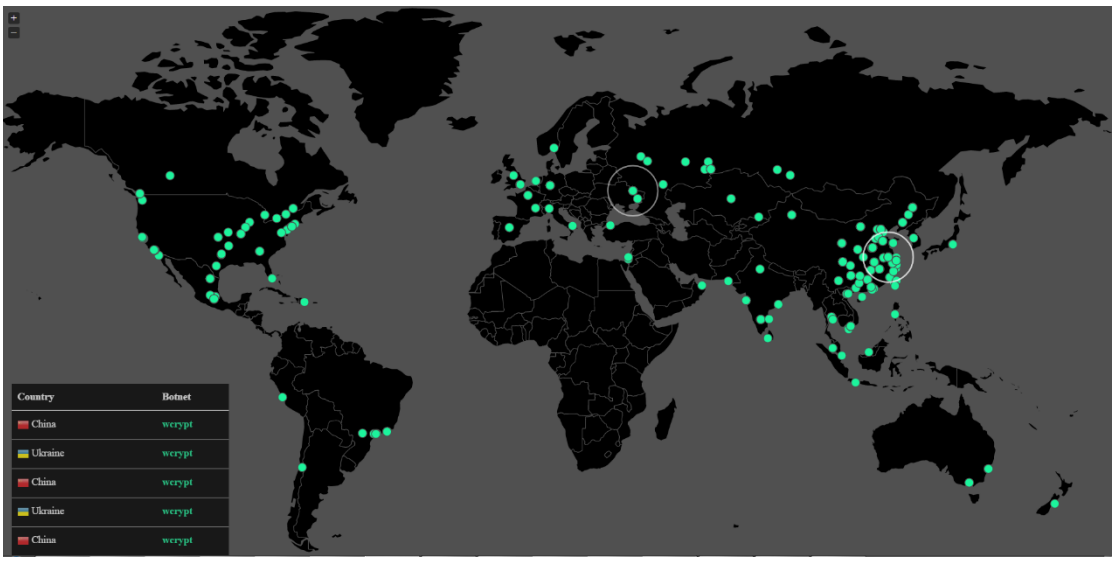


圖 2. (圖片來源截圖自 https://goo.gl/xgXiFZ)

為何此次 WannaCry 事件會如此的嚴重呢?傳統的勒索病毒軟體大部分都是透過點擊惡意連結、郵件附檔或 Flashplayer 等較為被動的方式散播，但是 WannaCry 除了以上的方法之外，還會利用 Windows SMB 的漏洞進行類似蠕蟲的主動式傳播行為，導致只要在區域網路中有一台主機中勒索病毒，會主動掃描區域網路中其他主機是否開啟 445 通訊埠，然後利用先前遭到外洩的美國 NSA 攻擊程式 EternalBlue 進行弱點滲透攻擊。

攻擊手法

駭客利用 CVE-2017-0144(SMB 漏洞)攻入目標主機，取得權限後下載木馬程式，並對區域網路和網際網路的任意主機進行連接埠掃描以擴大感染範圍，散播加密程式。中勒索病毒的主機也執行加密程式，使用的是 RSA 2048 和 CBC 模式 AES 加密文件內容，加密流程如圖 3 說明。

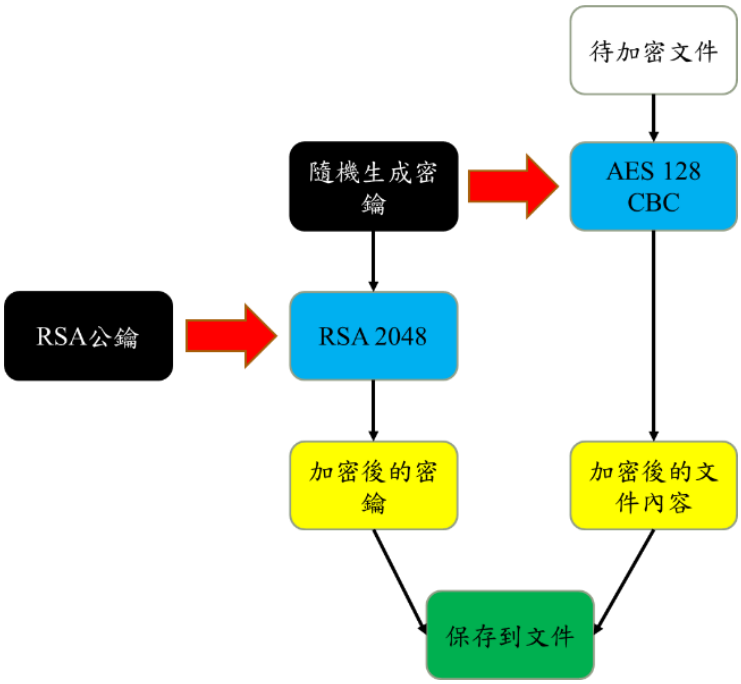


圖 3. (圖片參考自 https://goo.gl/vqh19l)

完成文件加密動作之後，惡意程式會產生勒索之說明文檔。圖 4 為病毒執行與散播的手法簡單說明。

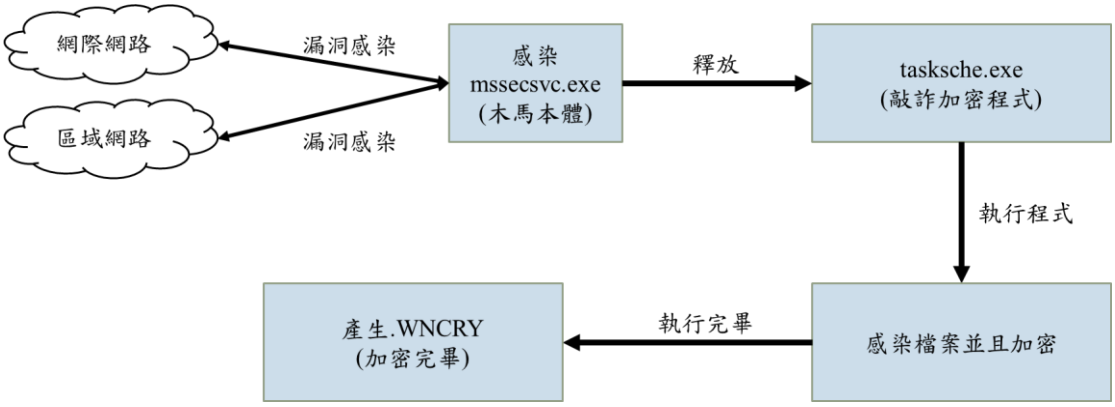


圖 4. (圖片參考自 https://goo.gl/vqh19l)

主機感染病毒之後，首先執行 mssecsvc.exe ，隨機對其他主機掃描 445 通訊埠，接著建立 tasksche.exe 程式，執行檔案加密及檔案刪除。

tasksche.exe 在執行檔案加密時，除了\ProgramData, \Program Files, \Program Files (x86), \Intel, \AppData\Local\Temp, \Local Settings\Temp, \WINDOWS 等需要維持系統運作的系統檔案資料夾不會被加密之外，其餘的檔案都會被複製一份後加密成附檔名為 .WNRCY 的檔案類型，被加密的原始檔案也將全部被刪除。

最後出現勒索的畫面，有各種語言版本如英文、俄文、簡體中文或繁體中文等等，勒索金額要價美金 300 元等值的比特幣，如三天內未支付贖金，金額將翻倍至 600 美金，如下圖 5 所示。

圖 5. WannaCry 勒索畫面

暫時性解決方案

由於勒索病毒的攻擊手法裡，包含了一項反分析機制，用以預防資安人員研究病毒的攻擊手法，而找出破解的方法。所以勒索病毒程式裡加入了一項判斷機制，利用向 DNS server 查詢某網域名稱是否已註冊，藉以確認是否可以進行攻擊。例如查詢網域名稱 iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com：

1. 如果 DNS server 回應此網域尚未註冊，則 WannaCry 勒索病毒會認為是安全的，可以繼續擴散。
2. 如果 DNS server 回應此網域的 IP 位址，WannaCry 病毒認定自己被放置於沙盒(Sandbox)測試環境中，便會停止攻擊與擴散行為，以防被研究人員分析破解。

由 Cisco 研究員分析勒索病毒的部分程式碼之中我們可以發現，如下列程式碼所示，它會自動連線至尚未註冊的網域。我們也可以從 DNS 查詢的狀況發現異常，如圖 6 所示。

```
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
```

圖 6. (圖片來源轉載自 https://goo.gl/Ep7kgJ)

英國資安公司一位成員注意到上述情況，註冊了被發現的尚未註冊的網域名稱，無意間造成全世界的 WannaCry 病毒都以為自己身處於沙盒(Sandbox)的測試環境中，而遏止了病毒大規模的擴散攻擊。

如下圖 7 所示，我們可以發現此網域已於 5/12 被註冊完畢。

```
Domain Name: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
Registrar: NAMECHEAP INC.
Sponsoring Registrar IANA ID: 1068
Whois Server: whois.namecheap.com
Referral URL: http://www.namecheap.com
Name Server: NS1.SINKHOLE.TECH
Name Server: NS2.SINKHOLE.TECH
Name Server: NS3.SINKHOLE.TECH
Name Server: NS4.SINKHOLE.TECH
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 12-may-2017
Creation Date: 12-may-2017
Expiration Date: 12-may-2018
```

圖 7. (圖片來源轉載自 https://goo.gl/Ep7kgJ)

新版 WannaCry

WannaCry 在 5/12~5/14 的周末肆虐全球打響名聲之後，專家們隨即開始研究防堵方法，讓用戶們能免受勒索病毒的攻擊，但駭客們也不是省油的燈，隔沒幾天，網路上就出現了新型的變種勒索病毒。

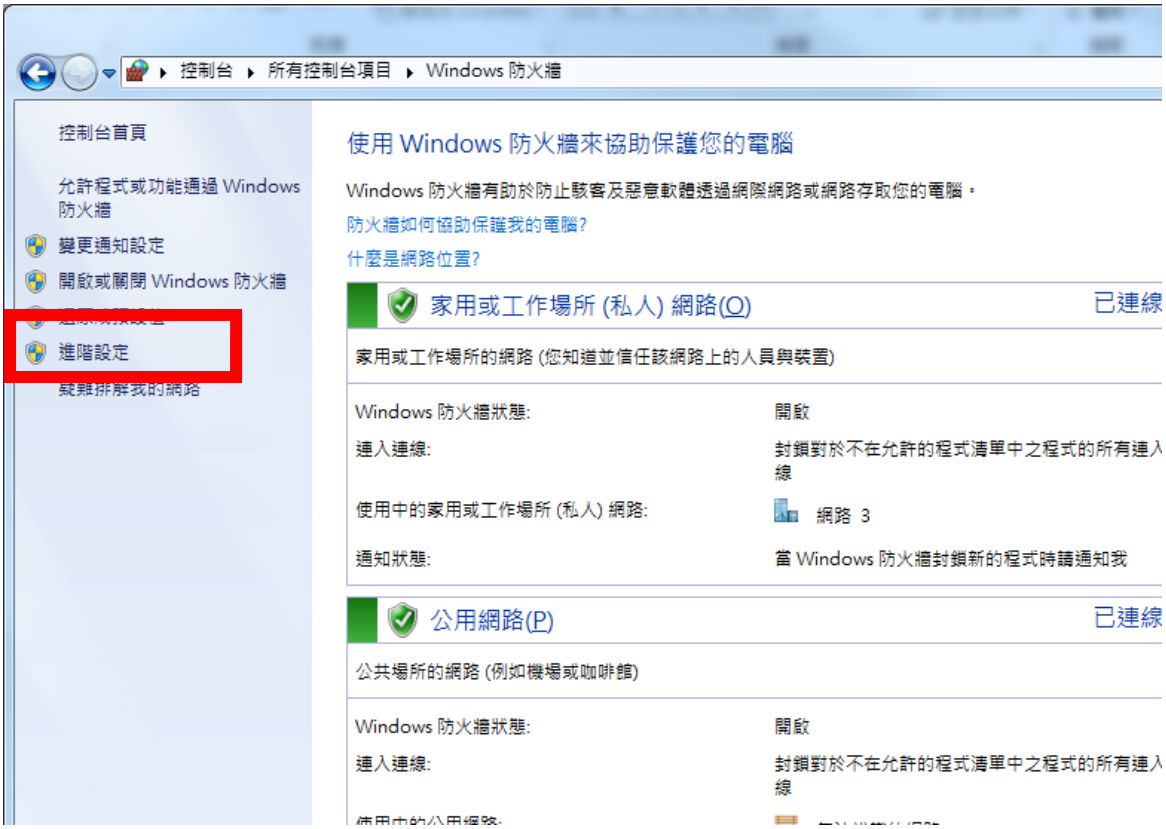
根據卡巴斯基實驗室指出，沒有「Kill Switch」(未註冊網域)機制的 WannaCry 病毒已經出現在網路上，但因為檔案有毀損，並沒有辦法完整執行功能，只能說是半成品，所以不構成威脅。

建議措施

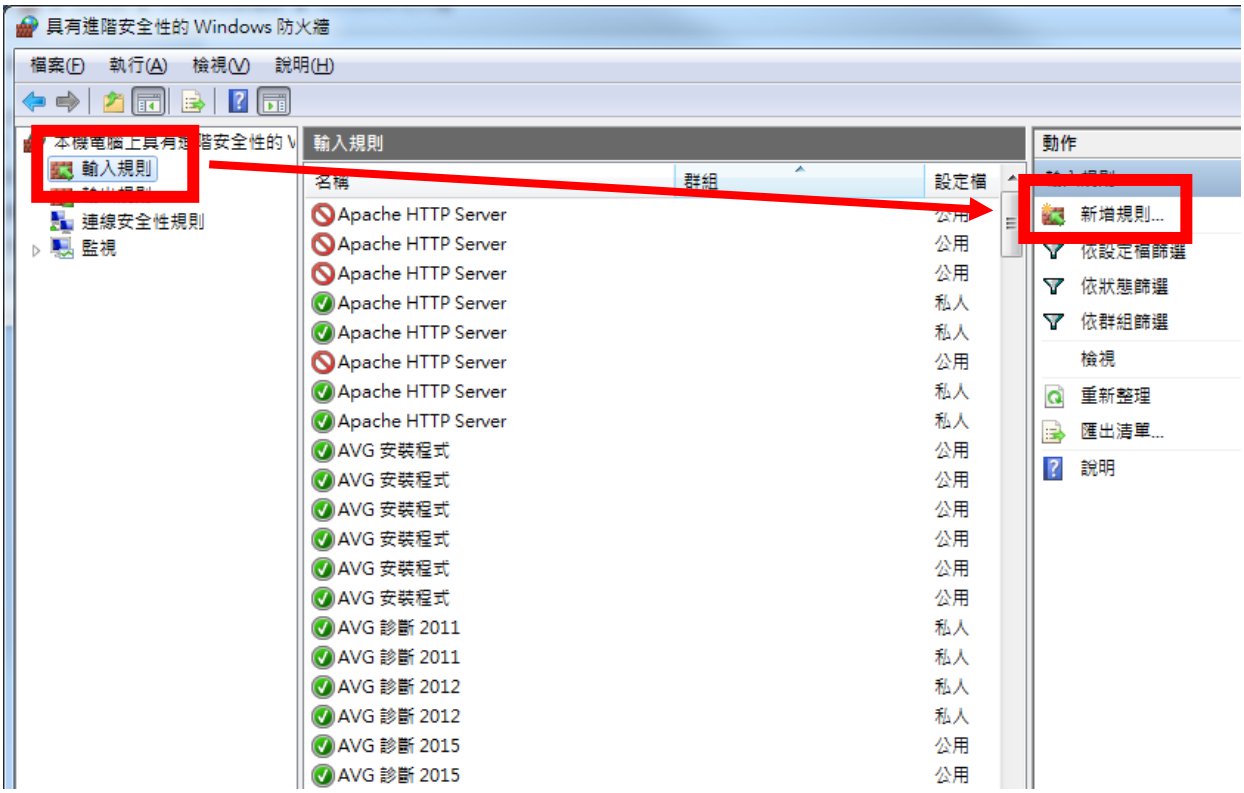
1. 開啟 Windows Update 更新微軟官方釋出的系統漏洞
2. 備份資料檔案(不須備份系統檔案)
3. 謹慎開啟網站連結與檔案
4. 安裝防毒軟體並維持病毒碼更新
5. 關閉主機 TCP 445 通訊埠（如下流程圖所示）

(1) 開啟控制台中的防火牆

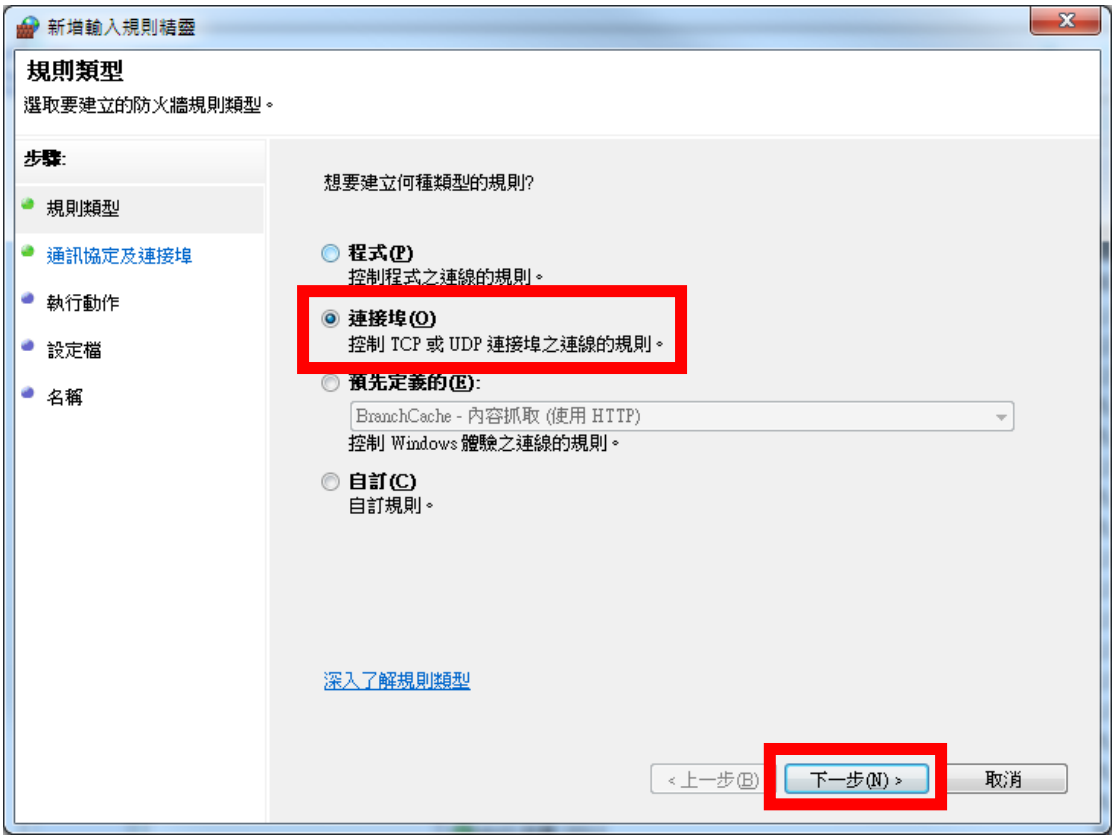
(2) 點選左邊欄位的「進階設定」



(3) 點選左邊欄位的「輸入規則」，點選右邊欄位的「新增規則」

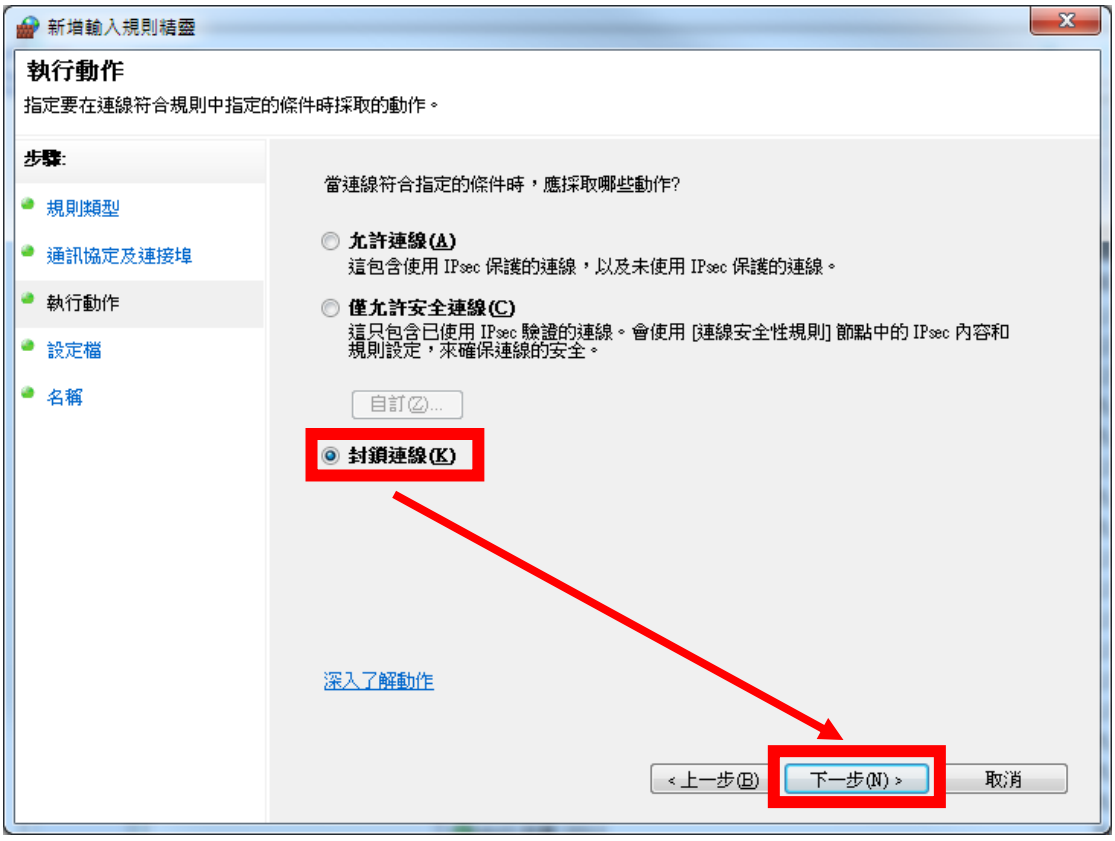


(4) 點選「連接埠」，點擊「下一步」

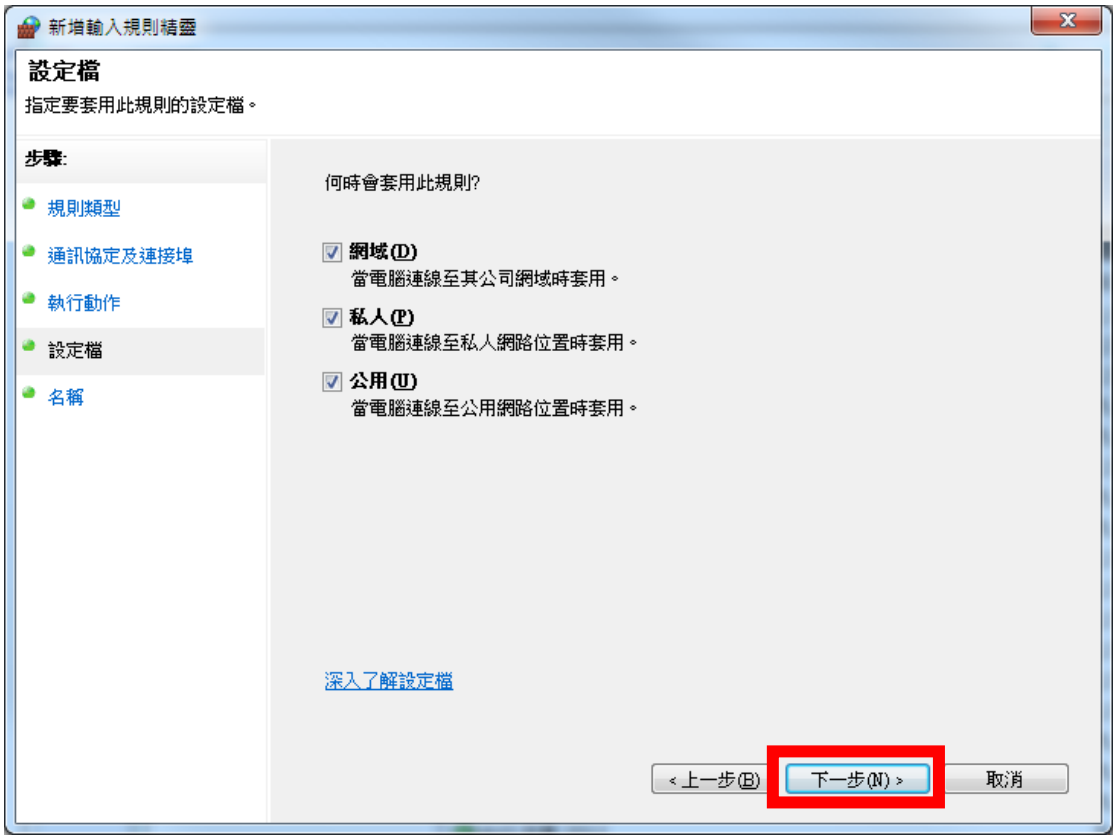


(5) 點選「TCP」，點選「特定本機連接埠」輸入 445，點擊「下一步」

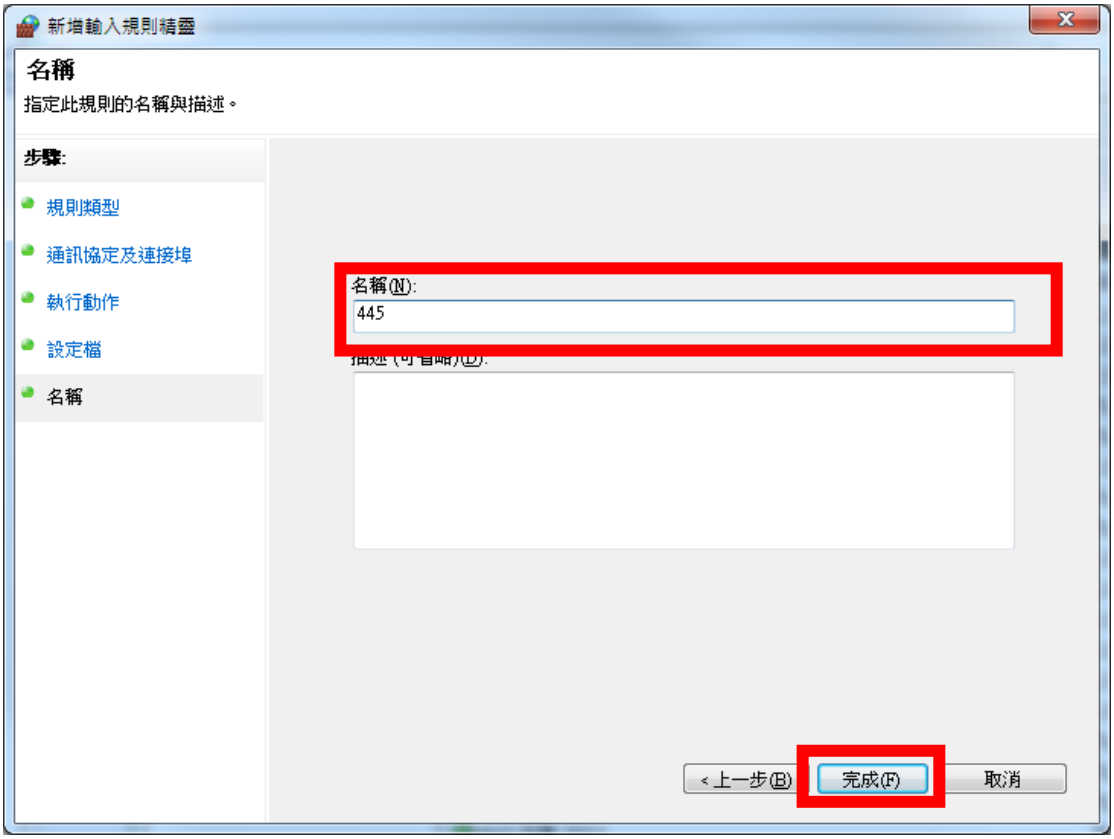
(6) 選取封鎖連線→按下一步



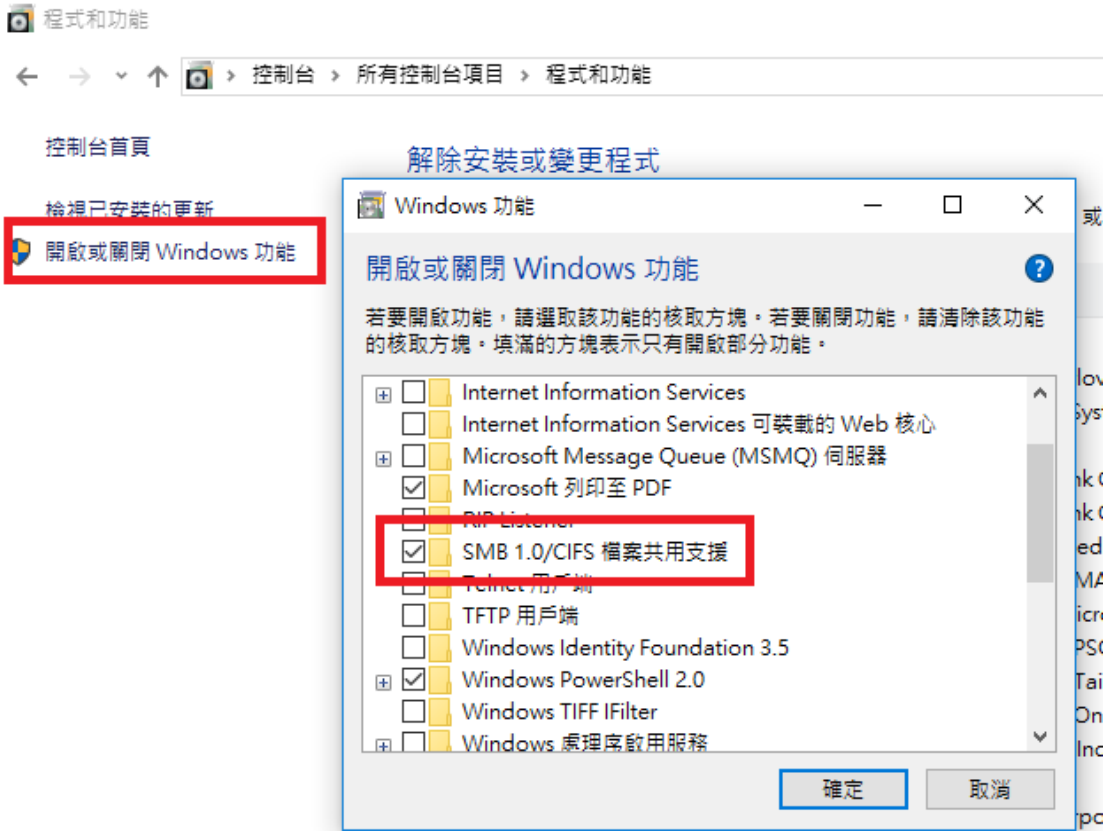
(7) 不需更改→按下一步



(8) 名稱輸入(如：445)→按完成



若自身沒有使用 SMB 的需求，也建議使用者可以到「新增/移除程式」裡面將服務給關閉，如下圖所示。



相關問題

根據卡巴斯基分析結果(如下圖所示)，被 WannaCry 勒索病毒攻擊成功的主機幾乎都是 Windows 7(所有版本合計占約 98%)，如圖 8 所示，雖然微軟已在今年 3 月釋出更新程式，但是因為 Windows 7 不像 Windows 10 會強制用戶系統更新，所以有許多主機因未能即時更新，遭受如 0day 一樣的攻擊，完全無法防禦。

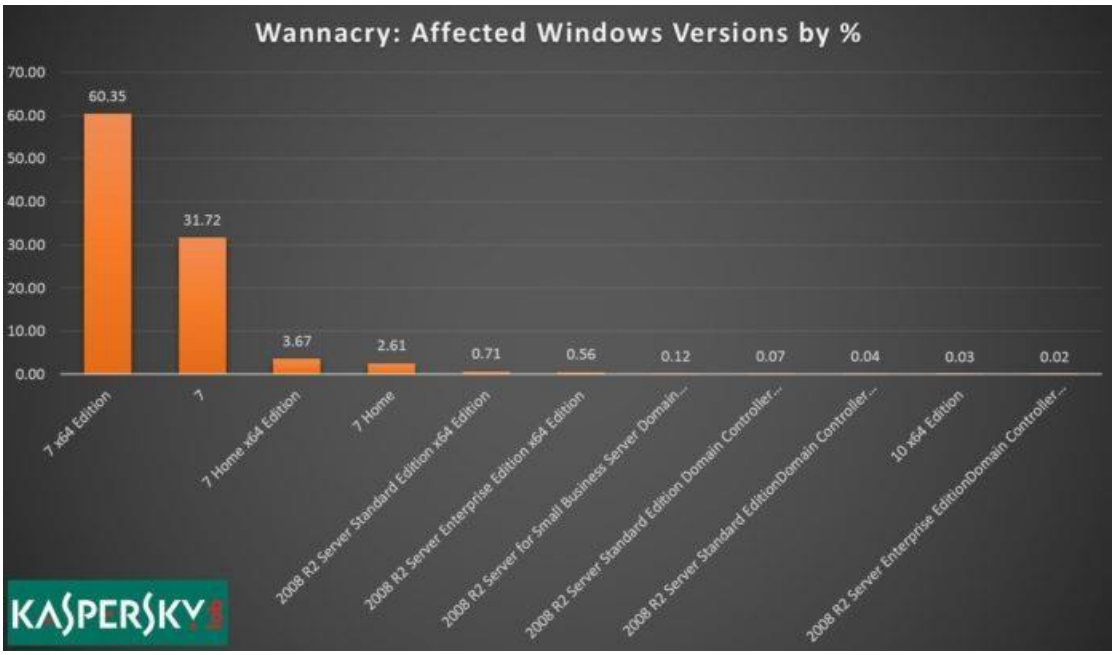


圖 8. (圖片來源轉載自 https://goo.gl/B38QXa)

我們經常會看到網路上的教學資訊，教大家不要開啟 Windows 更新，以免主機速度會變慢。然而此次來勢洶洶的勒索病毒攻擊，或許能讓大家思考，在現今資安議題日趨嚴重的時代，安全與方便或效能間的權衡，需要用不同的角度重新檢視才行。

參考資料

https://zh.wikipedia.org/wiki/WannaCry

https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

http://www.appledaily.com.tw/realtimenews/article/new/20170515/1118638/

https://unwire.hk/2017/05/21/wannacry-victim-statistics/tech-secure/

http://hitcon-girls.blogspot.tw/2017/05/wanacrypt0r-ransomware.html

https://twcert-official-file.s3.hicloud.net.tw/TWCERTCC-MIFR-2017001.pdf

http://blog.talosintelligence.com/2017/05/wannacry.html

https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

https://www.fireeye.com/blog/products-and-services/2017/05/wannacry-ransomware-campaign.html

https://intel.malwaretech.com/WannaCrypt.html

https://technews.tw/2017/05/16/new-wannacry/

http://tw.on.cc/tw/bkn/cnt/news/20170513/bkntw-20170513143203895-0513_04011_001.html