

預防 WanaCrypt0r 2.0 勒索病毒攻擊的方法

一、前言

近日勒索軟體 WanaCrypt0r 2.0 利用 Windows 系統的 SMB 漏洞，大規模的攻擊未安裝修正過後更新檔的 Windows 系統，而造成受害者系統上的檔案被加密，被加密的檔案副檔名都會變更為 .wncry，至目前為止絕大部分的受害者系統以 Windows XP、7 與 8.1 居多，建議使用相關系統的使用者，提高警覺並儘速安裝相關更新程式。

二、病毒資訊

NO	項目	內容
1	病毒名稱	WanaCrypt0r 2.0 (又名 WannaCry 或 Wcry)
2	微軟編號	MS17-010
3	CVE 編號	CVE-2017-0143、CVE-2017-0144、CVE-2017-0145、CVE-2017-0146、 CVE-2017-0148
4	病毒特徵	<p>「WanaCrypt0r 2.0」主要是透過 Windows 系統內名為 EternalBlue 的 Windows SMB 遠端執行程式碼弱點進行攻擊，而成功利用弱點的攻擊者則有機會獲得在目標伺服器上執行程式碼的能力。</p> <p>攻擊者成功攻擊該漏洞之後，可以將檔案送入受害系統，再將此檔案作為服務執行，接著再將真正的勒索病毒檔案送入受害系統，它會用 .WNCRY 副檔名來對檔案進行加密，同時也會送入另一個用來顯示勒索通知的檔案；被針對的副檔名包括 Microsoft Office、資料庫、壓縮檔、多媒體檔案和各種程式語言常用的副檔名。</p> <p>使用者電腦在遭受感染後，因電腦內檔案被加密成副檔名為 .WNCRY 的格式，導致受害者無法正常讀取檔案。檔案被加密後，該惡意軟體會鎖住電腦網路，並利用使用者的資料進行勒索，彈出紅色的勒索視窗，指示受害者需在 3 天內交付 300 美元的比特幣(Bitcoin)贖金，而後每兩個小時贖金增加 100 美元，一路增至 600 美元，若未能在 7 天內交付贖金、取得解密金鑰，則受害者將無法恢復電腦內的已被加密的檔案。</p>
5	受影響作業系統	Windows XP Windows Vista Windows7 Windows8 Windows8.1 Windows Server 2008 Windows Server 2008 R2

NO	項目	內容
		Windows Server 2012 Windows Server 2012 R2 Windows RT 8.1

三、建議措施

下面內容為針對 Windows 7 與 Windows 8.1 作業系統所進行的預防步驟說明，由於微軟公司已停止支援 Window XP 及 Windows Server 2003 系統的自動更新，建議使用此兩個系統的使用者可以到微軟公司的官方網站直接下載修補程式，並進行手動更新作業。微軟提供之更新檔案網址：

<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>。

1. 移除網路線或關閉無線網路，確認電腦未連接至網路。

由於 Wanacrypt0r 2.0 是透過 SMB 檔案分享的 TCP 445 連接埠來傳播，如果使用者的電腦可以跟辦公室內的其他電腦相連、互傳檔案的話(如:網路芳鄰)，就有機會被感染。



2. 關閉 Windows 系統的 445 通訊埠：



在未更新安全修正程式的情況下，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。下面為在 Windows 7 與 Windows 8.1 兩個作業系統內如何關閉 445 通訊埠的步驟說明。

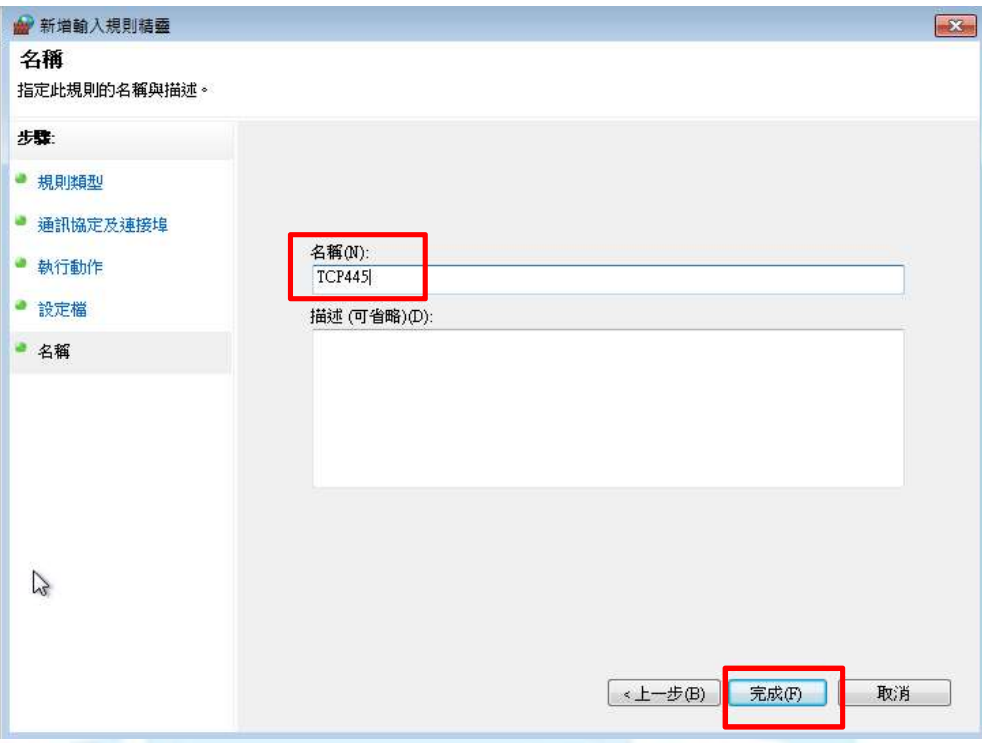


(1)Windows 7 關閉 445 通訊埠的方式：

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，設定方式如下：

No	說明	圖示
1	在防火牆之輸入規則設定頁面，點選視窗右邊區塊內，輸入規則之「新增規則」選項。	

No	說明	圖示
2	點選「連接埠」選項，並按「下一步」。	 <p>新增輸入規則精靈</p> <p>規則類型 選取要建立的防火牆規則類型。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 執行動作 設定檔 名稱 <p>想要建立何種類型的規則?</p> <p><input type="radio"/> 程式(P) 控制程式之連線的規則。</p> <p><input checked="" type="radio"/> 連接埠(O) 控制 TCP 或 UDP 連接埠之連線的規則。</p> <p><input type="radio"/> 預先定義的(E): BranchCache - 內容抓取 (使用 HTTP) 控制 Windows 體驗之連線的規則。</p> <p><input type="radio"/> 自訂(C) 自訂規則。</p> <p>深入了解規則類型</p> <p>< 上一步(B) 下一步(N) > 取消</p>
3	點選「TCP」選項，特定本機連接埠輸入 445，並按「下一步」。	 <p>新增輸入規則精靈</p> <p>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。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 執行動作 設定檔 名稱 <p>此規則會套用於 TCP 或 UDP?</p> <p><input checked="" type="radio"/> TCP(T)</p> <p><input type="radio"/> UDP(U)</p> <p>這個規則套用於所有本機連接埠或特定本機連接埠?</p> <p><input type="radio"/> 所有本機連接埠(A)</p> <p><input checked="" type="radio"/> 特定本機連接埠(S): 445 範例: 80, 443, 5000-5010</p> <p>深入了解通訊協定及連接埠</p> <p>< 上一步(B) 下一步(N) > 取消</p>

No	說明	圖示
4	點選「封鎖連線」，並按「下一步」。	 <p>新增輸入規則精靈</p> <p>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。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 執行動作 設定檔 名稱 <p>當連線符合指定的條件時，應採取哪些動作?</p> <ul style="list-style-type: none"> <input type="radio"/> 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。 <input type="radio"/> 僅允許安全連線 (C) 這只包含已使用 IPsec 驗證的連線。會使用 [連線安全性規則] 節點中的 IPsec 內容和規則設定，來確保連線的安全。 <input checked="" type="radio"/> 封鎖連線 (K) <p>自訂(O)...</p> <p>深入了解動作</p> <p>< 上一步(B) 下一步(N) > 取消</p>
5	確認所有網路環境都套用此規則，並且按「下一步」。	 <p>新增輸入規則精靈</p> <p>設定檔 指定要套用此規則的設定檔。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 執行動作 設定檔 名稱 <p>何時會套用此規則?</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> 網域 (D) 當電腦連線至其公司網域時套用。 <input checked="" type="checkbox"/> 私人 (P) 當電腦連線至私人網路位置時套用。 <input checked="" type="checkbox"/> 公用 (U) 當電腦連線至公用網路位置時套用。 <p>深入了解設定檔</p> <p>< 上一步(B) 下一步(N) > 取消</p>


No	說明	圖示																														
6	針對規則命名，建議名稱可與事件或規則內容有關，避免忘記其用途。輸入規則名稱為TCP445，並點選「完成」。	 <p>新增輸入規則精靈</p> <p>名稱 指定此規則的名稱與描述。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 執行動作 設定檔 名稱 <p>名稱(N): TCP445</p> <p>描述(可省略)(D):</p> <p>< 上一步(B) 完成(F) 取消</p>																														
7	完成後在「輸入規則」內會看到剛剛新增的規則 TCP445。	 <p>具有進階安全性的 Windows 防火牆</p> <p>檔案(F) 執行(A) 檢視(V) 說明(H)</p> <p>本機電腦上具有進階安全性的 Windows 防火牆</p> <p>輸入規則</p> <table border="1"> <thead> <tr> <th>名稱</th> <th>群組</th> <th>設定檔</th> <th>已啟用</th> <th>執行動作</th> </tr> </thead> <tbody> <tr> <td>TCP445</td> <td></td> <td>全部</td> <td>是</td> <td>封鎖</td> </tr> <tr> <td>BranchCache - 內容抓取 (HTTP-In)</td> <td>BranchCache - 內容抓取 (...)</td> <td>全部</td> <td>否</td> <td>允許</td> </tr> <tr> <td>BranchCache - 同儕節點探索 (WSD-In)</td> <td>BranchCache - 同儕節點探...</td> <td>全部</td> <td>否</td> <td>允許</td> </tr> <tr> <td>BranchCache - 託管快取伺服器 (HTTP-In)</td> <td>BranchCache - 託管快取伺...</td> <td>全部</td> <td>否</td> <td>允許</td> </tr> <tr> <td>HomeGroup 輸入</td> <td>HomeGroup</td> <td>私人</td> <td>否</td> <td>允許</td> </tr> </tbody> </table>	名稱	群組	設定檔	已啟用	執行動作	TCP445		全部	是	封鎖	BranchCache - 內容抓取 (HTTP-In)	BranchCache - 內容抓取 (...)	全部	否	允許	BranchCache - 同儕節點探索 (WSD-In)	BranchCache - 同儕節點探...	全部	否	允許	BranchCache - 託管快取伺服器 (HTTP-In)	BranchCache - 託管快取伺...	全部	否	允許	HomeGroup 輸入	HomeGroup	私人	否	允許
名稱	群組	設定檔	已啟用	執行動作																												
TCP445		全部	是	封鎖																												
BranchCache - 內容抓取 (HTTP-In)	BranchCache - 內容抓取 (...)	全部	否	允許																												
BranchCache - 同儕節點探索 (WSD-In)	BranchCache - 同儕節點探...	全部	否	允許																												
BranchCache - 託管快取伺服器 (HTTP-In)	BranchCache - 託管快取伺...	全部	否	允許																												
HomeGroup 輸入	HomeGroup	私人	否	允許																												
8	將 TCP 445 的輸入規則設定完成後，以同樣方式新增 UDP 445 的規則，兩者作法的差異之處如右圖所示，在規則類型的設定頁面，選「UDP」選項，在規格名稱的命名頁面輸入「UDP445」，其餘作法都相同。	 <p>新增輸入規則精靈</p> <p>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。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 執行動作 設定檔 名稱 <p>此規則會套用於 TCP 或 UDP?</p> <p><input type="radio"/> TCP (T)</p> <p><input checked="" type="radio"/> UDP (U)</p> <p>這個規則套用於所有本機連接埠或特定本機連接埠?</p> <p><input type="radio"/> 所有本機連接埠(A)</p> <p><input checked="" type="radio"/> 特定本機連接埠(S): 445 範例: 80, 443, 5000-5010</p> <p>深入了解通訊協定及連接埠</p> <p>< 上一步(B) 下一步(N) > 取消</p>																														

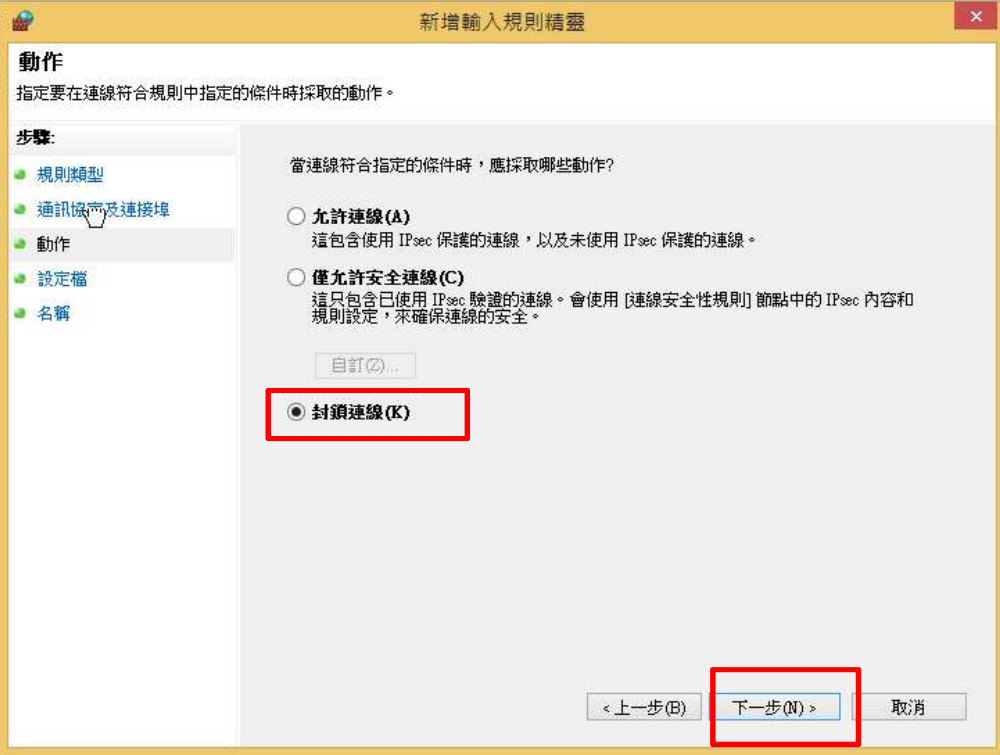
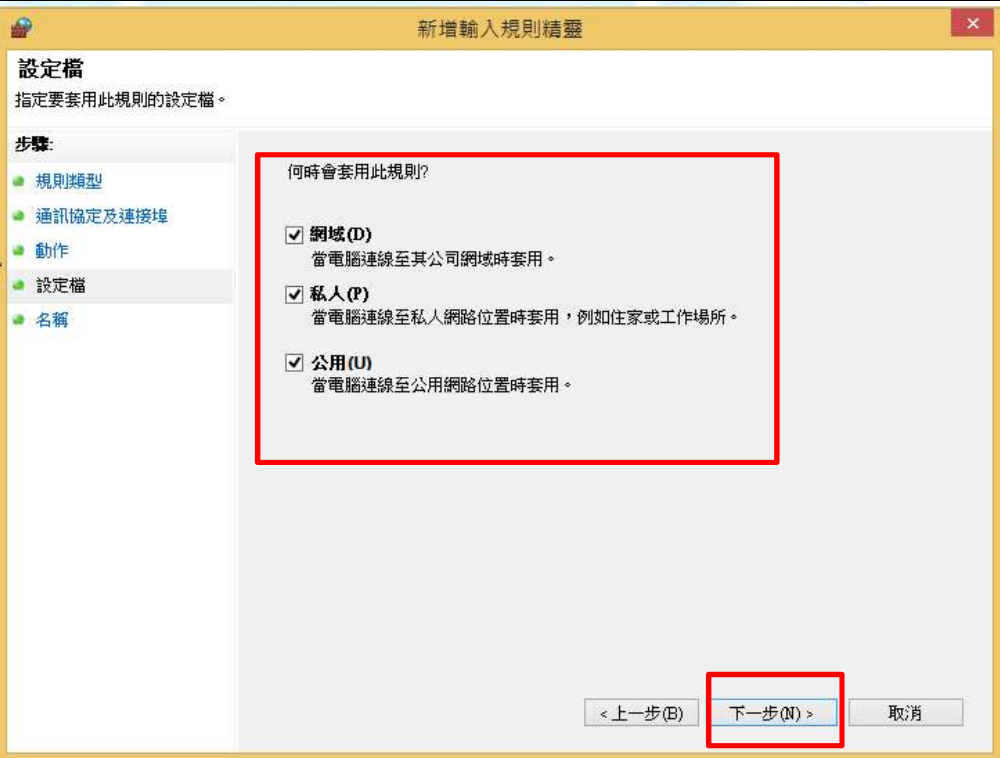
No	說明	圖示
9	設定完成後，會在「輸入規則」區塊內看到兩條新增規則：TCP445 與 UDP445。	

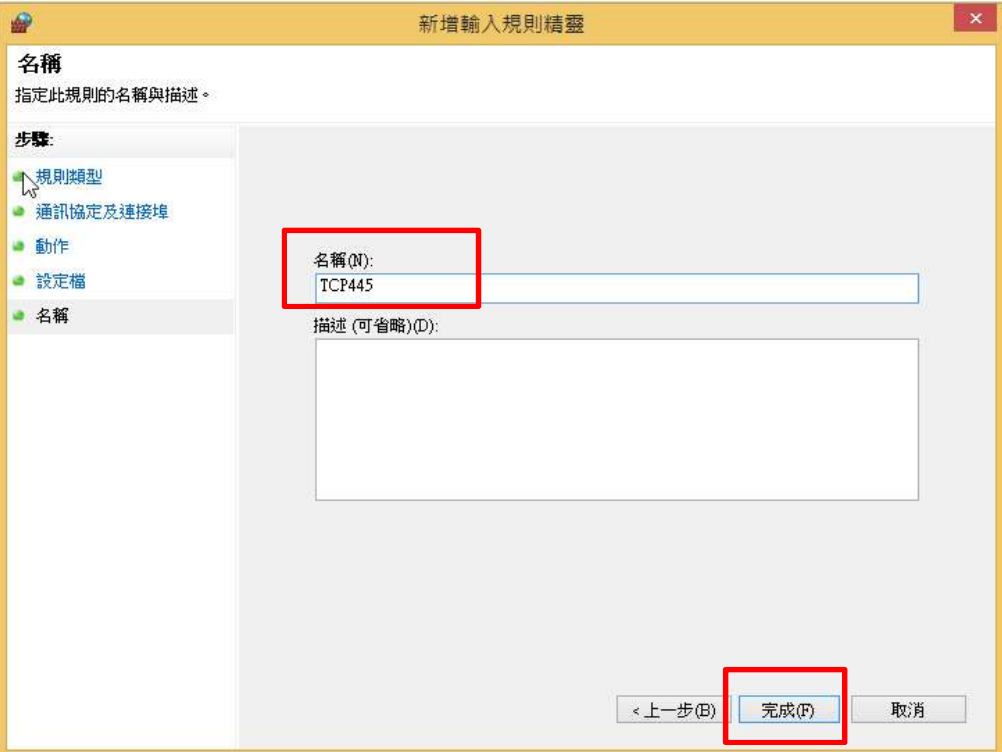
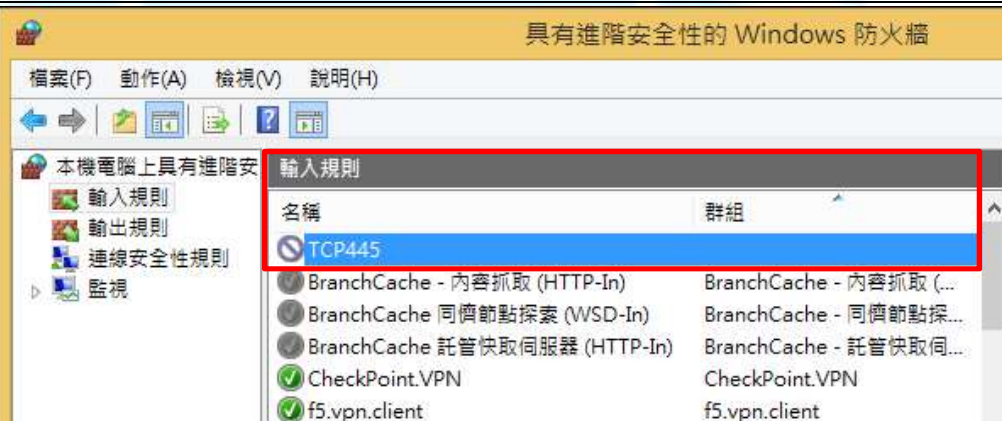
(2)Windows 8.1 關閉 445 通訊埠的方式::



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，設定方式如下:

NO	說明	圖示
1	在防火牆「輸入規則」頁面視窗之最右區塊內，點選「新增規則」選項。	

NO	說明	圖示
2	<p>點選「連接埠」選項，並按「下一步」。</p>	 <p>新增輸入規則精靈</p> <p>規則類型 選取要建立的防火牆規則類型。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 動作 設定檔 名稱 <p>想要建立何種類型的規則?</p> <ul style="list-style-type: none"> <input type="radio"/> 程式(P) 控制程式之連線的規則。 <input checked="" type="radio"/> 連接埠(O) 控制 TCP 或 UDP 連接埠之連線的規則。 <input type="radio"/> 預先定義的(E): BranchCache - 內容抓取 (使用 HTTP) 控制 Windows 體驗之連線的規則。 <input type="radio"/> 自訂(C) 自訂規則。 <p>< 上一步(B) 下一步(N) > 取消</p>
3	<p>點選「TCP」選項，特定本機連接埠輸入 445，並按「下一步」。</p>	 <p>新增輸入規則精靈</p> <p>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。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 動作 設定檔 名稱 <p>此規則會套用於 TCP 或 UDP?</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> TCP(T) <input type="radio"/> UDP(U) <p>這個規則套用於所有本機連接埠或特定本機連接埠?</p> <ul style="list-style-type: none"> <input type="radio"/> 所有本機連接埠(A) <input checked="" type="radio"/> 特定本機連接埠(S): 445 範例: 80, 443, 5000-5010 <p>< 上一步(B) 下一步(N) > 取消</p>

NO	說明	圖示
4	點選「封鎖連線」，並按「下一步」。	 <p>新增輸入規則精靈</p> <p>動作 指定要在連線符合規則中指定的條件時採取的動作。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 動作 設定檔 名稱 <p>當連線符合指定的條件時，應採取哪些動作？</p> <ul style="list-style-type: none"> <input type="radio"/> 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。 <input type="radio"/> 僅允許安全連線(C) 這只包含已使用 IPsec 驗證的連線。會使用 [連線安全性規則] 節點中的 IPsec 內容和規則設定，來確保連線的安全。 <input checked="" type="radio"/> 封鎖連線(K) <p>自訂(O)...</p> <p>< 上一步(B) 下一步(N) > 取消</p>
5	確認所有網路環境都套用此規則，並且按「下一步」。	 <p>新增輸入規則精靈</p> <p>設定檔 指定要套用此規則的設定檔。</p> <p>步驟:</p> <ul style="list-style-type: none"> 規則類型 通訊協定及連接埠 動作 設定檔 名稱 <p>何時會套用此規則？</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> 網域(D) 當電腦連線至其公司網域時套用。 <input checked="" type="checkbox"/> 私人(P) 當電腦連線至私人網路位置時套用，例如住家或工作場所。 <input checked="" type="checkbox"/> 公用(U) 當電腦連線至公用網路位置時套用。 <p>< 上一步(B) 下一步(N) > 取消</p>

NO	說明	圖示
6	<p>針對規則命名，建議名稱可與事件或規則內容有關，避免忘記其用途。輸入規則名稱為TCP445，並點選「完成」。</p>	 <p>The screenshot shows the '新增輸入規則精靈' (New Rule Wizard) dialog box. The '名稱' (Name) field contains 'TCP445'. The '完成(F)' (Finish) button is highlighted with a red box.</p>
7	<p>完成後在「輸入規則」內會看到剛剛新增的規則 TCP445。</p>	 <p>The screenshot shows the '具有進階安全性的 Windows 防火牆' (Windows Firewall with Advanced Security) window. The '輸入規則' (Inbound Rules) list is expanded, and the rule 'TCP445' is highlighted with a red box.</p>

NO	說明	圖示																														
8	<p>將 TCP 445 的輸入規則設定完成後，以同樣方式新增 UDP 445 的規則，兩者作法的差異之處如右圖所示，在規則類型的設定頁面，選「UDP」選項，在規格名稱的命名頁面輸入「UDP445」，其餘作法都相同。</p>	 <p>The figure consists of two screenshots from the Windows Firewall rule wizard. The first screenshot, titled '新增輸入規則精靈' (New Input Rule Wizard), shows the '通訊協定及連接埠' (Communication and Connection) step. It asks '此規則會套用到 TCP 或 UDP?' (This rule will apply to TCP or UDP?) with 'UDP (U)' selected. Below, it asks '這個規則套用到所有本機連接埠或特定本機連接埠?' (This rule applies to all local connections or specific local connections?) with '特定本機連接埠 (S):' (Specific local connections) selected and the value '445' entered. The second screenshot shows the '名稱' (Name) step, where the name '名稱 (N):' is set to 'UDP445'.</p>																														
9	<p>設定完成後，會在「輸入規則」區塊內看到兩條新增規則：TCP445 與 UDP445。</p>	 <p>The figure shows a screenshot of the Windows Firewall console titled '具有進階安全性的 Windows 防火牆' (Windows Firewall with Advanced Security). The '輸入規則' (Inbound Rules) list is visible, showing two newly added rules: 'UDP445' and 'TCP445'. Both rules are set to '全部' (All) for scope, '是' (Yes) for enabled, and '封鎖' (Block) for action.</p> <table border="1" data-bbox="718 1556 1476 1742"> <thead> <tr> <th>名稱</th> <th>群組</th> <th>設定權</th> <th>已啟用</th> <th>動作</th> </tr> </thead> <tbody> <tr> <td>UDP445</td> <td></td> <td>全部</td> <td>是</td> <td>封鎖</td> </tr> <tr> <td>TCP445</td> <td></td> <td>全部</td> <td>是</td> <td>封鎖</td> </tr> <tr> <td>BranchCache - 內容抓取 (HTTP-In)</td> <td>BranchCache - 內容抓取 (...)</td> <td>全部</td> <td>否</td> <td>允許</td> </tr> <tr> <td>BranchCache 同儕節點探索 (WSD-In)</td> <td>BranchCache - 同儕節點探...</td> <td>全部</td> <td>否</td> <td>允許</td> </tr> <tr> <td>BranchCache 託管快取伺服器 (HTTP-In)</td> <td>BranchCache - 託管快取伺...</td> <td>全部</td> <td>否</td> <td>允許</td> </tr> </tbody> </table>	名稱	群組	設定權	已啟用	動作	UDP445		全部	是	封鎖	TCP445		全部	是	封鎖	BranchCache - 內容抓取 (HTTP-In)	BranchCache - 內容抓取 (...)	全部	否	允許	BranchCache 同儕節點探索 (WSD-In)	BranchCache - 同儕節點探...	全部	否	允許	BranchCache 託管快取伺服器 (HTTP-In)	BranchCache - 託管快取伺...	全部	否	允許
名稱	群組	設定權	已啟用	動作																												
UDP445		全部	是	封鎖																												
TCP445		全部	是	封鎖																												
BranchCache - 內容抓取 (HTTP-In)	BranchCache - 內容抓取 (...)	全部	否	允許																												
BranchCache 同儕節點探索 (WSD-In)	BranchCache - 同儕節點探...	全部	否	允許																												
BranchCache 託管快取伺服器 (HTTP-In)	BranchCache - 託管快取伺...	全部	否	允許																												

3. 備份電腦內重要資料。

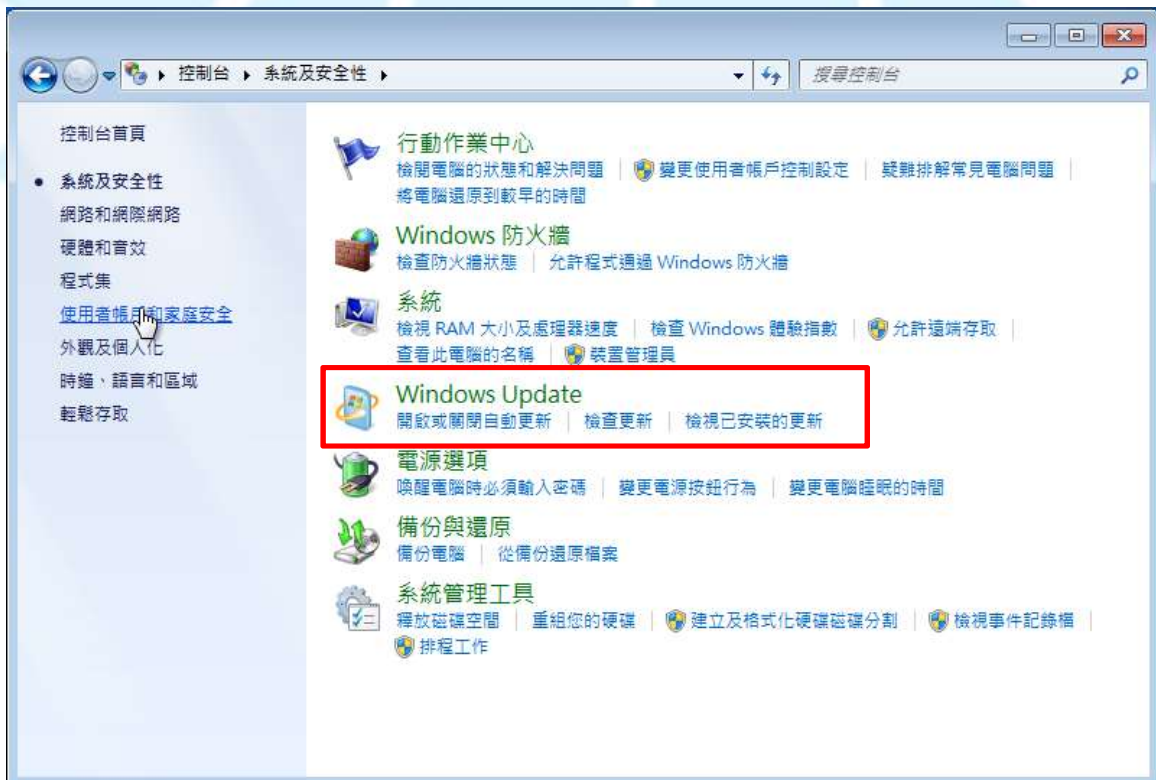
4. 重新開啟網路連線，使電腦可連上網際網路。

5. 使用 Windows Update 更新或手動更新微軟 KB4012215(漏洞編號 MS17-010)：

為了避免電腦在尚未更新系統時，被其他已中毒的電腦攻擊，故在更新前我們先做一層防護，將 445 通訊埠關閉，在確認攻擊者無法透過此連接埠進入後，我們開始進行系統更新作業。下面為針對 Windows 7 與 Windows 8.1 兩個作業系統進行系統更新的詳細步驟說明。

(1)在 Windows 7 內執行 Windows update 的更新方式：

在「控制台」>「系統及安全性」頁面內，點選「Windows Update」，進行「檢查更新」，確認已安裝最新的系統更新檔。



(2)在 Windows 8.1 內執行 windows update 的更新方式：

在「控制台」>「系統及安全性」頁面內，點選「Windows Update」，進行「檢查更新」，確認已安裝最新的系統更新檔。



(3) 手動更新微軟 KB4012215(漏洞編號 MS17-010)的方式：
至微軟官方網站下載修補程式進行更新，參考網址如下。

KB4012215：

<https://support.microsoft.com/zh-tw/help/4012215>

MS17-010：

<https://technet.microsoft.com/zh-tw/library/security/ms17-010.aspx?f=255&MSPPError=-2147217396#ID0EHB>

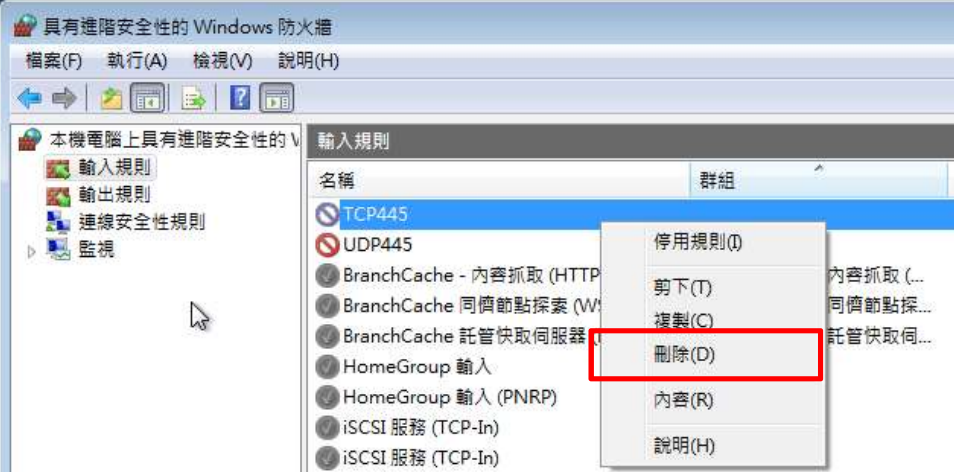
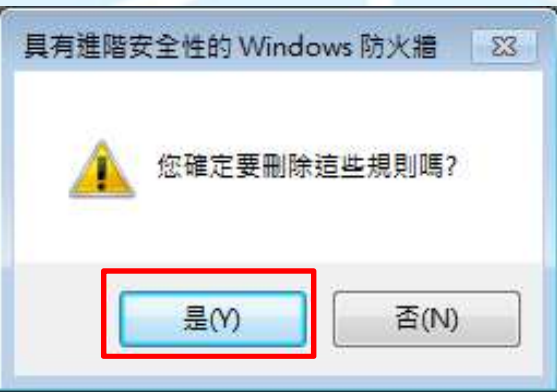
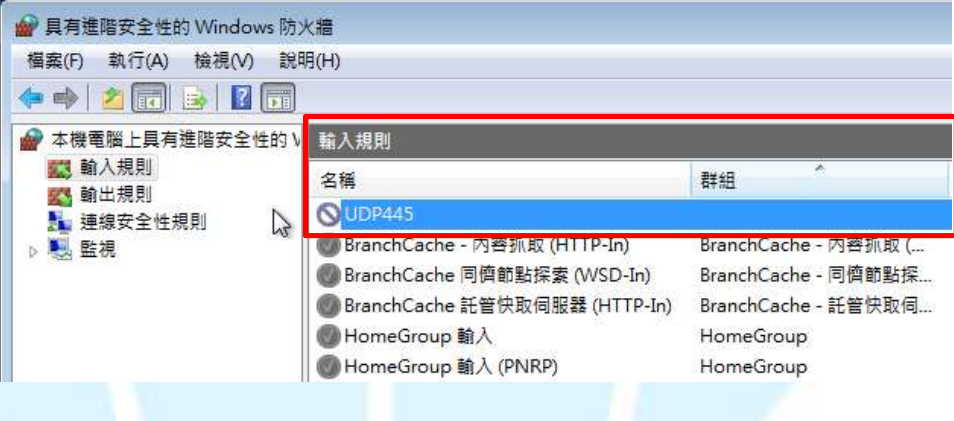
6. 更新電腦內之防毒軟體與病毒碼。

為了更有效預防 Wanacrypt0r 2.0 勒索病毒的攻擊，建議使用者至微軟官方網站下載、安裝微軟免費防毒軟體 Windows Defender，因為目前 Windows Defender 已經可以針對系統中的惡意程式 Wanacrypt0r 2.0 提供偵測並清除。

7. 重新開啟 445 通訊埠的連線功能：

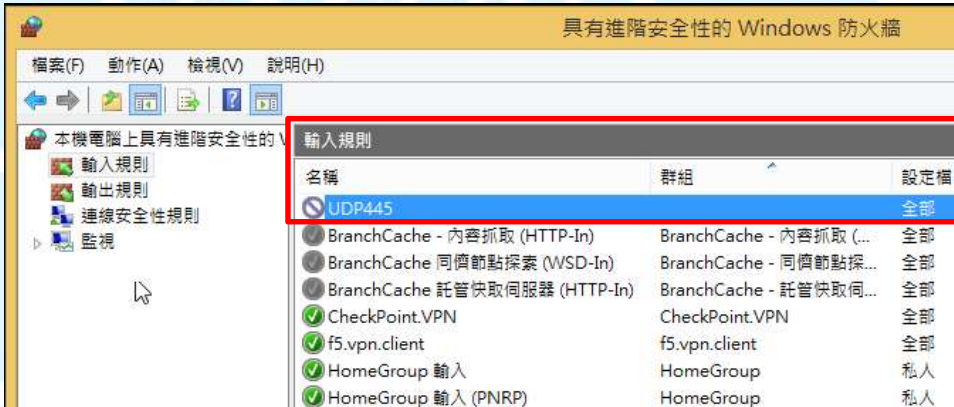
(1)Windows 7 重開 445 連接埠的方式：

NO	說明	圖示
----	----	----

NO	說明	圖示
1	點選「輸入規則」之 TCP445 規則，並按滑鼠右鍵，出現選項方塊後，點選「刪除」選項。	 <p>The screenshot shows the Windows Firewall control panel window. On the left, the 'Input Rules' folder is expanded. In the main list, the 'TCP445' rule is selected. A right-click context menu is open over this rule, with the 'Delete (D)' option highlighted by a red rectangle.</p>
2	出現是否刪除規則的詢問視窗後，點選「是」。	 <p>The screenshot shows a confirmation dialog box titled '具有進階安全性的 Windows 防火牆'. The message asks '您確定要刪除這些規則嗎?' (Are you sure you want to delete these rules?). There are two buttons: '是 (Y)' (Yes) and '否 (N)' (No). The 'Yes' button is highlighted with a red rectangle.</p>
3	完成後，我們可以發現輸入規則內已無 TCP445 的規則，接著以同樣方式進行 UDP445 規則的刪除動作。	 <p>The screenshot shows the Windows Firewall control panel window. The 'Input Rules' folder is expanded. In the main list, the 'UDP445' rule is selected and highlighted with a blue background. A red rectangle is drawn around the entire rule list area.</p>

(2)Windows 8.1 內重開 445 連接埠的方式:

NO	說明	圖示
----	----	----

NO	說明	圖示
1	點選「輸入規則」之 TCP445 規則，並按滑鼠右鍵，出現選項方塊後，點選「刪除」選項。	 <p>The screenshot shows the Windows Firewall console with the 'Input Rules' tab selected. The 'TCP445' rule is highlighted, and a context menu is open over it. The 'Delete (D)' option is highlighted with a red box.</p>
2	出現是否刪除規則的詢問視窗後，點選「是」。	 <p>The screenshot shows a confirmation dialog box titled '具有進階安全性的 Windows 防火牆'. The message asks '您確定要刪除這些規則嗎?' (Are you sure you want to delete these rules?). The 'Yes (Y)' button is highlighted with a red box.</p>
3	完成後，我們可以發現輸入規則內已無 TCP445 的規則，接著以同樣方式進行 UDP445 規則的刪除動作。	 <p>The screenshot shows the Windows Firewall console with the 'Input Rules' tab selected. The 'UDP445' rule is now highlighted with a blue selection bar, and it is circled with a red box. The 'TCP445' rule is no longer visible in the list.</p>

在執行完成以上步驟後，建議使用者可以至下列網站進行系統漏洞之安全檢查。
線上檢查網站：<https://doublepulsar.below0day.com/>

參考資料：

1. <https://www.facebook.com/twcertcc/posts/1947829248780144>
2. <https://www.facebook.com/twcertcc/posts/1947904648772604>
3. <https://www.facebook.com/MicrosoftTaiwan/posts/1024724287627679:0>
4. <http://technews.tw/2017/05/13/ransomware-wanacrypt0r-2/>
5. <https://blog.trendmicro.com.tw/?p=49682>