完全防範 WannaCry（WanaCrypt0r）勒索病毒處理流程（官方解法整理版）

微軟在「MS17-010」安全公告中的「因應措施」一節提供了能夠避免遭到威脅的方法，本文參考微軟官方提供的因應措施，以確保電腦安全！

Step 1. 中斷網路連線

如果不確定電腦是否已經免疫，請先將網路連線中斷，這個步驟建議必做。

Step 2. 停用 SMBv1 服務

WannaCry 能夠入侵使用者電腦，就是利用 Microsoft Server Message Block 1.0（SMBv1）的弱點進行攻擊，請參考下官方建議停用 SMBv1 服務，避免遭到攻擊。

適用於執行 Windows 8.1 或 Windows Server 2012 R2 及更新版本的客戶的替代方法

- 若為用戶端作業系統：

(一)

1. 開啟 [**控制台**]，按一下 [**程式集**]，然後按一下 [**開啟或關閉 Windows 功能**]。
2. 在 [Windows 功能] 視窗中，清除 [**SMB 1.0/CIFS 檔案共用支援**] 核取方塊，然後按一下 [**確定**] 以關閉視窗。
3. **重新啟動系統**。

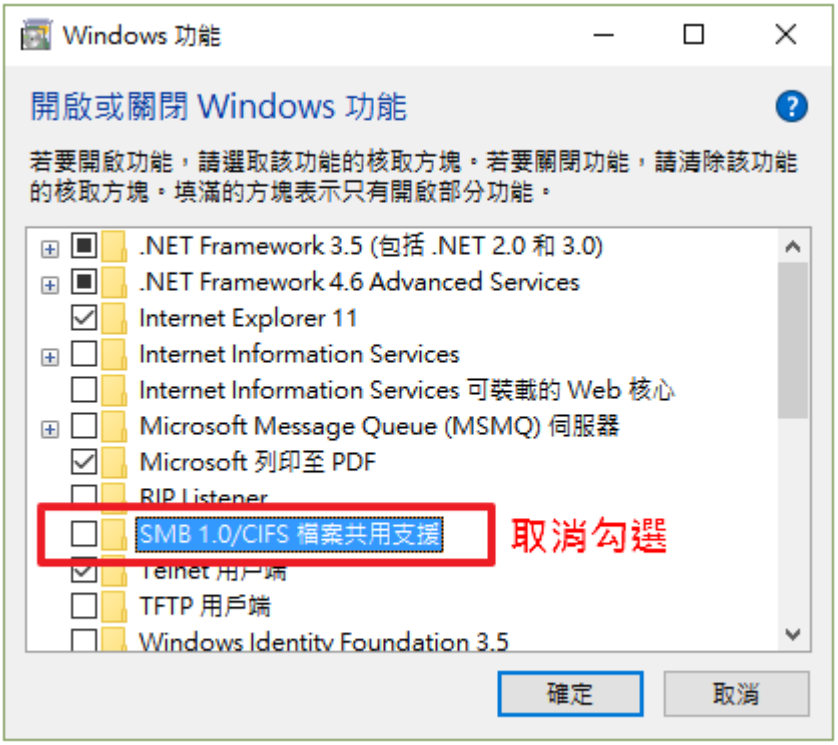
- 若為伺服器作業系統：

(一)

1. 開啟 [**伺服器管理員**]，然後按一下 [**管理**] 功能表並選取 [**移除角色及功能**]。
2. 在 [功能] 視窗中，清除 [**SMB 1.0/CIFS 檔案共用支援**] 核取方塊，然後按一下 [**確定**] 以關閉視窗。
3. **重新啟動系統**。

Windows 10

1. 點擊左下角的[**放大鏡**]圖式進行搜尋，輸入【**控制台**】
2. 按一下 [**程式集**]，然後按一下 [**開啟或關閉 Windows 功能**]。
3. 在 [Windows 功能] 視窗中，清除 [**SMB 1.0/CIFS 檔案共用支援**] 核取方塊，然後按一下 [**確定**] 以關閉視窗。
4. **重新啟動系統**。



▲ 關閉 SMB 1.0 功能

Windows 7

Windows 7 必須透過修改登錄機碼（registry）的方式才能停用 SMBv1。若您熟悉機碼修改方式，可以修改以下機碼進行停用/啟用：

機碼位置:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
機碼名稱：SMB1
REG_DWORD: 0 = 停用
REG_DWORD: 1 = 啟用（預設）

若您不熟悉機碼修改方式，可下載以下快速設定檔，解壓縮後執行「停用 SMBv1.reg」，**執行完成後同樣需重新啟動系統**。

下載關閉 Windows 7 SMBv1 快速設定檔

Step 3.（接上網路）立刻安裝更新檔並打開 Windows Update

依所使用 Windows 各版本的安裝更新檔：

- Windows 7：4 月份更新(32 位元、64 位元)、5 月份更新（32 位元、64 位元）
- Windows 8.1：4 月份更新(32 位元、64 位元)、5 月份更新（32 位元、64 位元）
- Windows XP、Vista：修補更新檔(2017/5/13 更新)

以上檔案皆為微軟官方載點，過程中如果需要重新啟動，請直接重新啟動，不要流連忘返！

安裝完獨立更新檔後，請依步驟打開 Windows Update：
1.點選左下角【開始】並選擇齒輪圖示進入【設定】視窗
2.選取［更新與安全性］ 功能
3.選擇選單左側的［Windows Update］並確認已經開啟
4.手動點擊【檢查更新】，確保電腦已安裝所有更新檔

Step 4. 安裝防毒軟體

目前已經有多家防毒軟體（含微軟系統內建）表示可偵測 WannaCry（WanaCrypt0r 2.0）勒索病毒，包含：ESET、Norton、Avast、Emsisoft、微軟，可優先安裝這些防毒軟體。

Step 5. 恢復網路連線