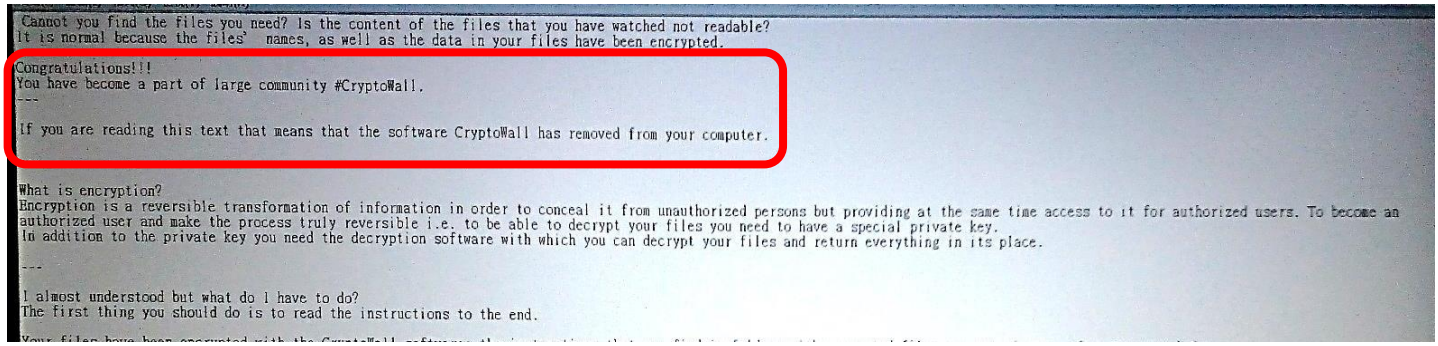
勒索軟體 CrytoWall 後續觀察記錄

剛剛再仔細看了一下相關的搜尋結果，發現如果你的圖檔是 PNG 應該沒事，因為病毒自行產生的圖檔格式就是 PNG。

另外突然發現有 TXT 文字檔，而且只在該**「使用者的桌面」和「C:\Users\該使用者\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup」下會發現「HELP_YOUR_FILES.TXT」檔**，其他產生的都是名為「HELP_YOUR_FILES」的圖檔。

這是告訴我們圖檔用 PNG，文字用 TXT 嗎？應該不是！不過在文字檔裡面有一句話**「If you are reading this text that means that the software CrytoWall has removed from your computer.」**



最近案例：

天兵工程師點「免費iPhone」釣魚信，竟害公司差點倒閉！| ...
oops.udn.com/.../1319615-天兵工程師點「免費iPhone」釣魚信，竟害...
2015年11月17日 - 惡名昭彰的CryptoLocker病毒，最近在台灣也傳出不少災情，這類軟體的特色是會將硬碟內所有檔案加密，藉此勒索苦主匯款救回檔案，恐怖之處 ...

加密勒索惡意軟體 Crypt0L0cker, CryptoLocker, CryptoWall 目前無解

感染惡意軟體的方法：

1. **FALSH 或 JAVA 漏洞：**駭客先把惡意軟體放在某個網頁，只要瀏覽到這個網頁，惡意軟體就利用 FASH 和 JAVA 的漏洞植入惡意軟體，開始加鎖電腦檔案。
2. **利用郵件夾帶 PDF 檔：**只要開啟感染惡意軟體的 PDF 檔，開始加鎖電腦檔案。

（參考網址：加密勒索惡意軟體 Crypt0L0cker, CryptoLocker, CryptoWall 目前無解。
http://hope11188.pixnet.net/blog/post/45514234-%E5%8A%A0%E5%AF%86%E5%8B%92%E7%B4%A2%E6%83%A1%E6%84%8F%E8%BB%9F%E9%AB%94-crypt0l0cker,-cryptolocker,-cryptow ）

簡易的防勒索病毒的方式

這是家瑜老師找到的方式「**PTT 神人輩出　鄉民撰寫萬用偵測勒索病毒腳本**」，主要的原理是利用「勒索病毒」會到磁碟開始搜尋相關符合的檔案類型，開始進行加密更改檔名的行為，所以**在磁碟機下放置一個「圖檔（誘餌）」，然後用個語法每 30 秒鐘去判斷這個圖檔在不在，如果不再就強制將電腦主機關機。**

這樣做的好處是避免病毒持續感染其他檔案，但是如果是你自己不小心誤刪掉該檔案，一樣會自動關機喔！而且經過測試，如果當你按下登入到電腦開機可以使用超過 30 秒，會發現電腦一直關機，因為找不到該檔案！

如果真的發現中了「勒索病毒」，透過這個方式關機後，該怎麼處理呢？

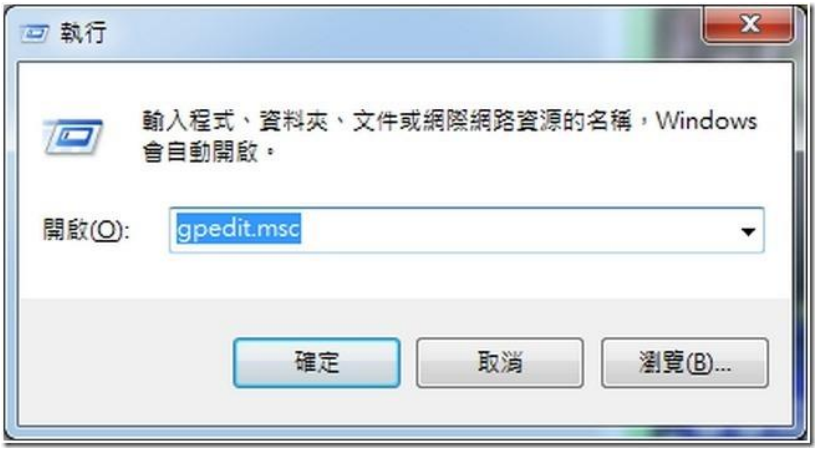
建議：將硬碟拔下來，透過外接的方式，使用另外一台電腦（這一台電腦建議先把資料除區離線，或者使用 LINUX 或 MAC 的主機)去開啟，然後把資料備份到另外一顆 HDD。

簡易防止的操作說明：

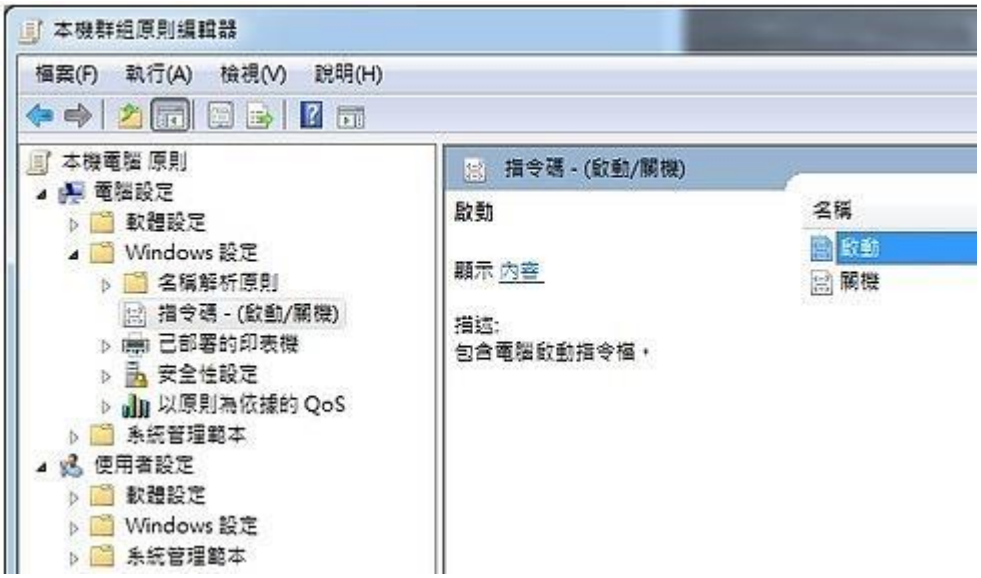
1. **首先下載該腳本和圖檔（M:\06 安裝光碟區\其他\防勒索簡易方法），裡面有 3 個檔案**

檔名	用途
vvvfku-c	如果希望 C 碟也偵測的話，將這個檔案和 1.jpg 一起複製到 C 碟貼上
vvvfku	如果希望 D 碟也偵測的話，將這個檔案和 1.jpg 一起複製到 D 碟貼上
1.JPG	預設的圖檔，我換成學校的校徽

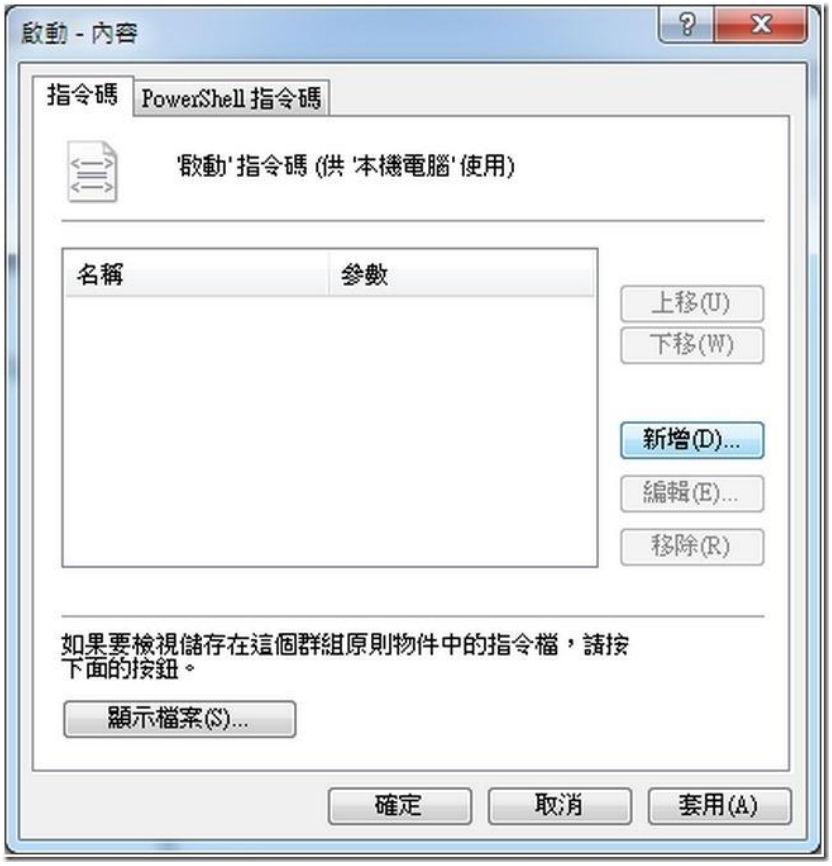
2. **開始→執行（輸入 gpedit.msc）**



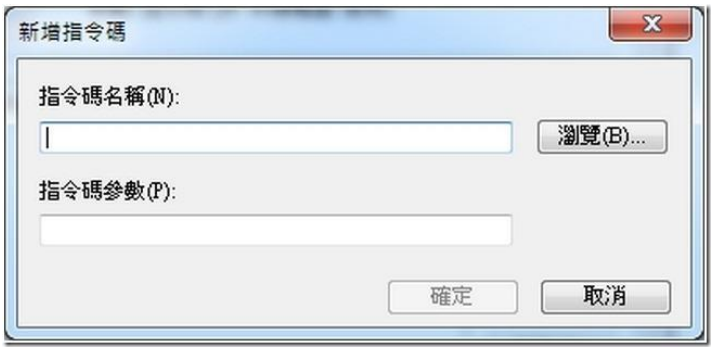
3. 找到「電腦設定」→「Windows 設定」→「指令碼-(啟動/關機)」→在右方的「啟動」點滑鼠左鍵 2 下



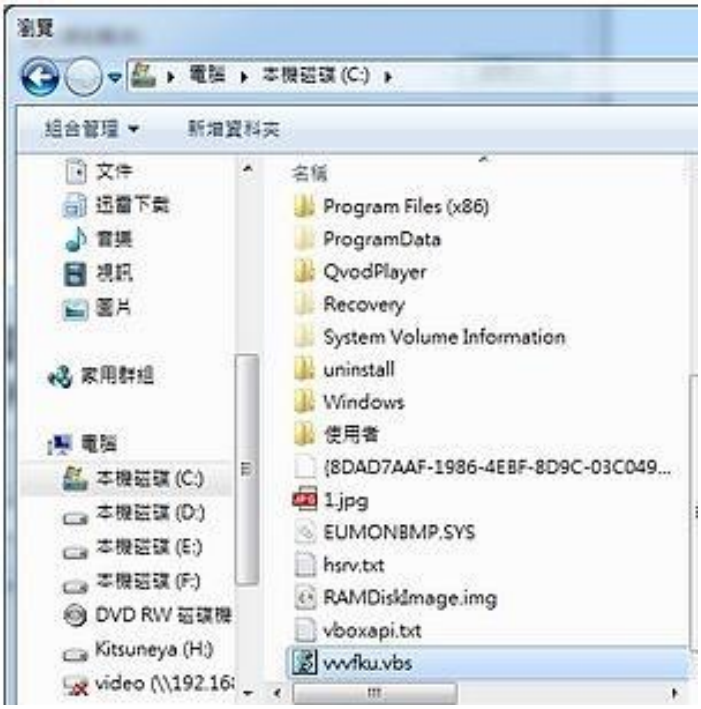
4. 按下「新增」



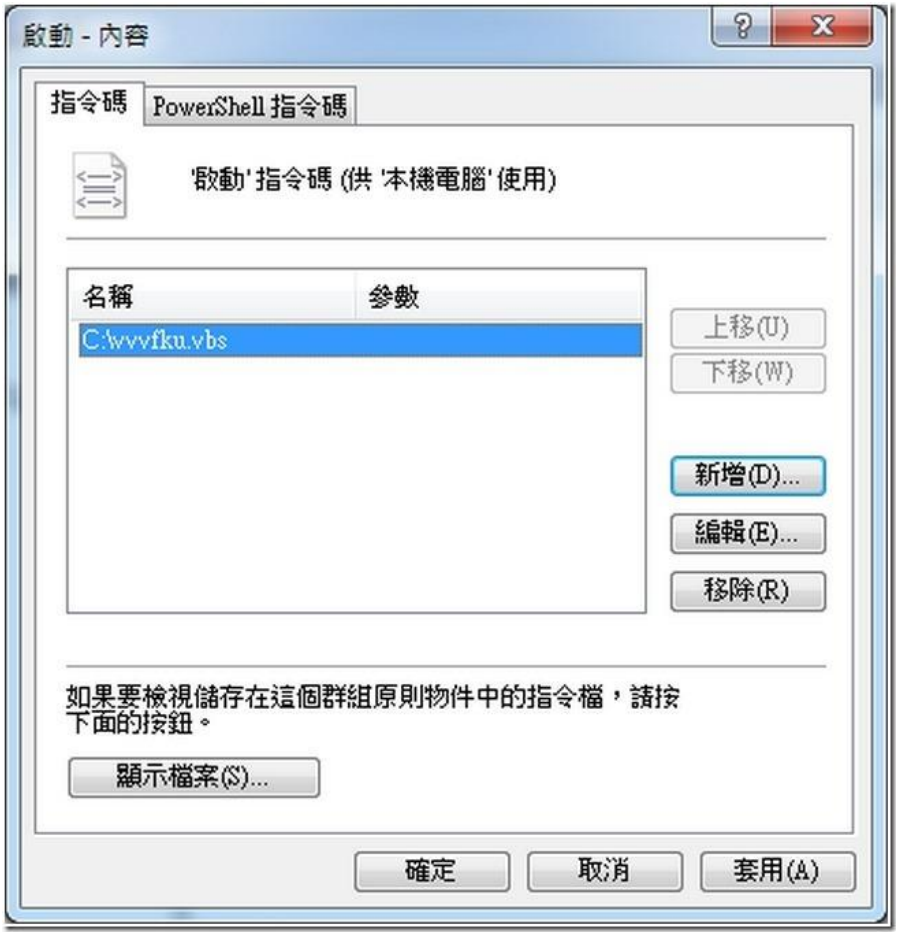
5. 在「指令碼名稱」選擇「瀏覽」



6. **找到「C 或 D 碟下的 vvvfku.vbs（或 vvvfku-c.vbs）」**



7. **確定後重新開機，就會存在這個規則了。**



因為這次觀看 HELP_YOUR_FILES.PNG 這個圖檔產生的時間，D 碟的時間比較早，所以我把 vvvfku.vbs，的內容改成去找「d:\1.jpg」

所以如果希望 C 碟也去搜尋的話，我複製一個同樣的檔案，名稱為「vvvfku-c.vbs」，這個要放在 C 碟下，所以新增的動作要做 2 次喔！

(PS：相關的操作圖片擷取自「PTT 神人輩出　鄉民撰寫萬用偵測勒索病毒腳本」。)

PS：只要使用這個方式，千萬千萬千萬千萬不要將「1.jpg」刪除或更名或搬到其他資料夾，如果不小心刪掉了，會很麻煩的！

真的不小心誤刪 1.jpg，開機又關機怎麼辦？

- 因為無法正常開機，所以必須要在開機後，**按「F8」進去後，選擇「安全模式（網路和指令模式....）」，在指令模式（黑底白字）的視窗下**，
- 不小心刪掉 C 碟下 1.jpg 的複製檔案方式：**Copy　c:\source\1.jpg　　c:**
- 不小心刪掉 D 碟下 1.jpg 的複製檔案方式：**Copy　c:\source\1.jpg　　d:**

PS：可以這樣處理的原因是因為，先前已經 1.jpg 複製到每一台電腦「c:\source」下，所以是自己的電腦，先在 C 碟見一個「source」的資料夾，把 1.jpg 複製到 source 下。

另外在社群上，有老師提供了另外一個方式「**[教學] 勒索軟體 3 秒鐘即時偵測 CryptoLocker 或 Crypt0L0cker - 以 Directory Monitor 為例**」是透過「Directory Monitor」這套軟體去監控重新命名的這個動作，當發現有檔案被重新命名的時候，會在右下角的工作列，跳出「檔案已重新命名」的提示。

根據勒索病毒的話，個人認為提示的時候，如果人不在電腦旁邊，會持續感染其他檔案，反而是上面的方法「關機」比較好！

但是如果是平常的時候，可以透過監控，來看看是否有其他不明的連線者，偷連到你的電腦，更改你的資料。