20170613_新的USB病毒_解決方式_v0.3

by 維修室/駐點林工程師提供.

Ref.: 資料來源: https://www.ptt.cc/bbs/NTUST_Talk/M.1370194255.A.FAE.html (2013/06/03)

1. 當你發現USB檔案都變成捷徑時，請不要執行任何東西，
萬一你已經點了，請照下面步驟做，如果還好沒點任何東西請跳到步驟3。

2. 如果你點了捷徑，那麼毒已經進入電腦，請先打開工作管理員 (CTRL+ALT+DEL)，然後切換到第二分頁「處理程序」
關閉運行中的wscript.exe，如果沒有就跳過。

3. 打開USB資料夾，去「組合管理」裡面找到「資料夾和搜尋選項」，
然後前往「檢視」分頁滑到最下面將三個「隱藏.....」的選項取消勾勾 (Vista僅兩個)，並且選擇「顯示隱藏的檔案、資料夾及磁碟機」。

4. 回到USB資料夾，此時你應該可以看到原有的檔案以及他的捷徑(被病毒創造的)。
把loopqa資料夾、autorun.inf資料夾、ynrhgwssck..vbs，以及所有捷徑刪除。

5. 到桌面左下角的開始，在搜尋欄輸入cmd，可以找到cmd.exe，請對他點選右鍵，
以管理員身分執行。如果沒有直接左鍵執行即可。

6. 這時候會跳出一個黑色視窗，請輸入：attrib -H -S (USB槽英文字母):*.*
例如我的USB是F槽： attrib -H -S F:*.*
請注意格式要正確，不要遺漏空格。
這個步驟是還原被病毒更動的檔案屬性。

7. 接下來請到 C:\Users\(使用者名稱)\AppData\Roaming\
Microsoft\Windows\Start Menu\Programs\Startup\
找到並刪除 ynrhgwssck..vbs，如果你一開始沒有執行捷徑的話不會產生。

8. 接著請到C:\Users\(使用者名稱)\AppData\Local\Temp\，
找到並刪除 system.wsf。

9. 最後到桌面左下角的開始，在搜尋欄打上 msconfig.exe，並且點擊
打開他，切換到「啟動」分頁將「Microsoft (R) Windows Script Host」打勾取消。
點選「套用」然後按下「確定」。到這裡解毒步驟完成，此時會請你重新啟動電腦，
建議重新啟動。

請勿刪除wscript.exe，他是Windows內建工具，只是被病毒借用了，依照步驟 8、9即可解除。

10. (選擇性)依照步驟3將原先的隱藏設定改回去，以免更動到重要檔案。

11.這時候你的USB應該就沒有問題了，試著把檔案複製進去/插拔USB，應該都不會
自動產生捷徑了。