

USB 隨身碟.lnk 捷徑病毒 v0.3 (圖文步驟指引文件)

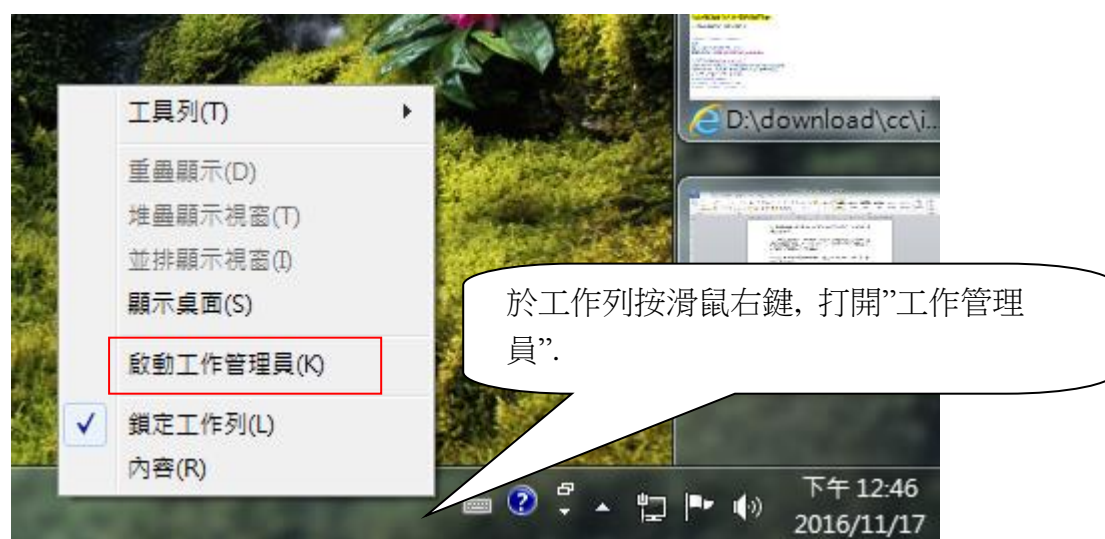
1. 說明:

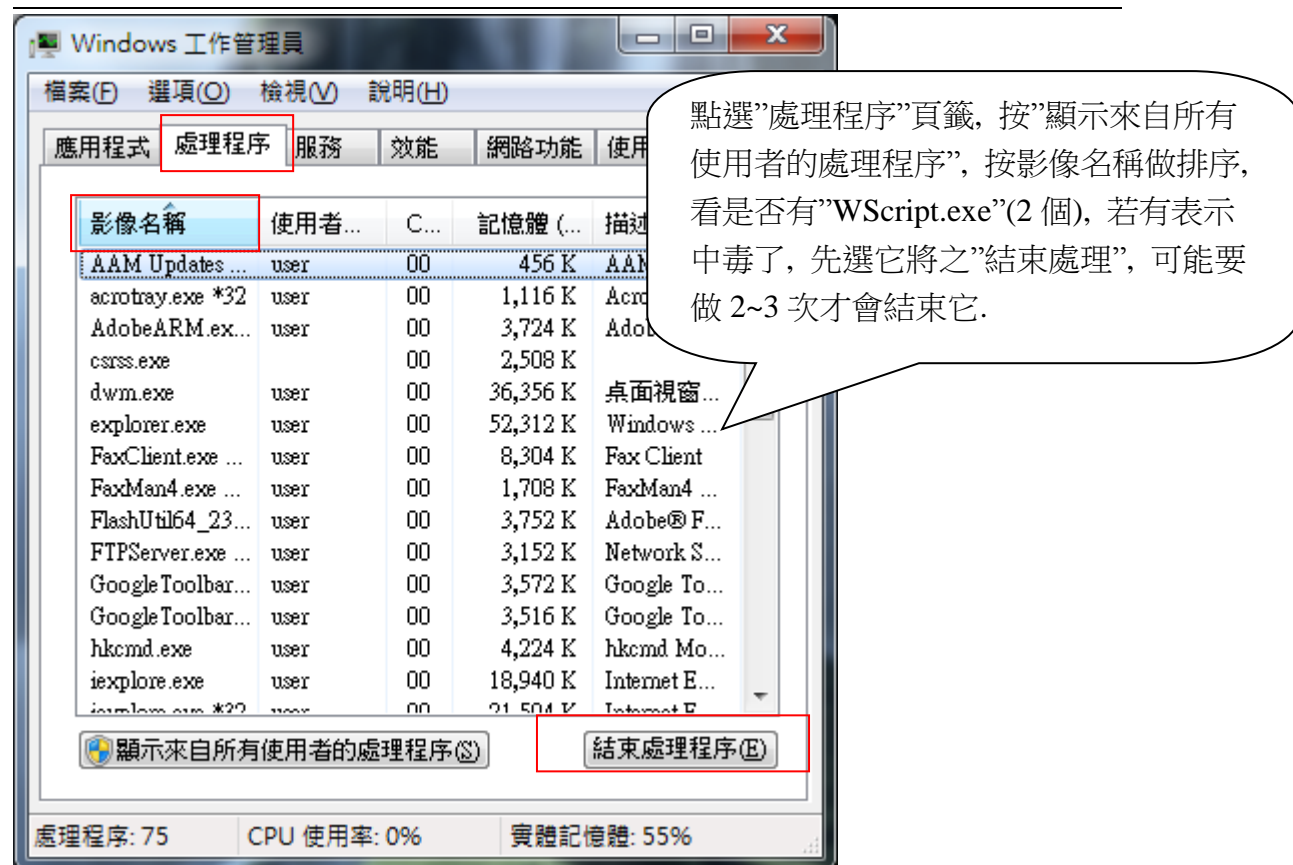
- 1.1 2016 年 6 月 21 日因資安通報(AISAC-84104)意外發現老師電腦中 USB 隨身碟.lnk 捷徑病毒.
- 1.2 .lnk 捷徑病毒特徵: 受感染的 USB 隨身碟目錄, 只有一個*.lnk 捷徑檔, 而原來的檔案被隱藏放入目錄為”_”內, 使用者有點擊.lnk 捷徑檔, 雖可看到原來的檔案, 但這樣就會將病毒再傳染給主機, 故千萬不要點.
- 1.3 另外, 受感染的 USB 隨身碟, 還多了隱藏目錄”WindowsServices”, 內有隱藏檔案 helper.vbs, installer.vbs, movemenoreg.vbs.
- 1.4 .lnk 捷徑病毒感染方式: 使用者有點選執行 USB 內的.lnk 捷徑檔, 雖可看到原來的檔案, 但這樣就中毒了, 且同時傳染至電腦或筆電主機, 造成交叉感染, 未來有任何 USB 隨身碟, 插入該中毒主機, 會將病毒傳給 USB, 反之亦然, 病毒有再生之能力.

2. .lnk 捷徑病毒處理方式:


2.1 必須確認主機本身沒有中毒, 才能處理中毒的 USB 隨身碟, 不然永遠清不完. 確認及清除方式:

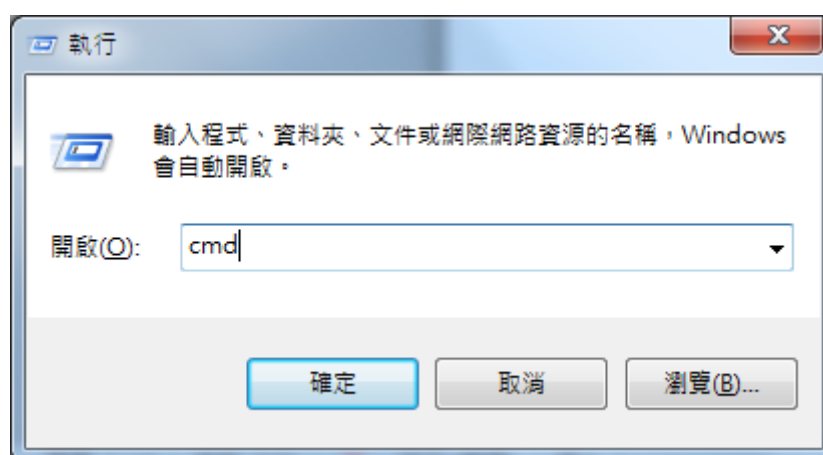
2.1.1 打開”工作管理員”->”處理程序”, 按”顯示來自所有使用者的處理程序”, 按影像名稱做排序, 看是否有”WScript.exe”(2 個), 若有表示中毒了, 先選它將之”結束處理”, 可能要做 2~3 次才會結束它.

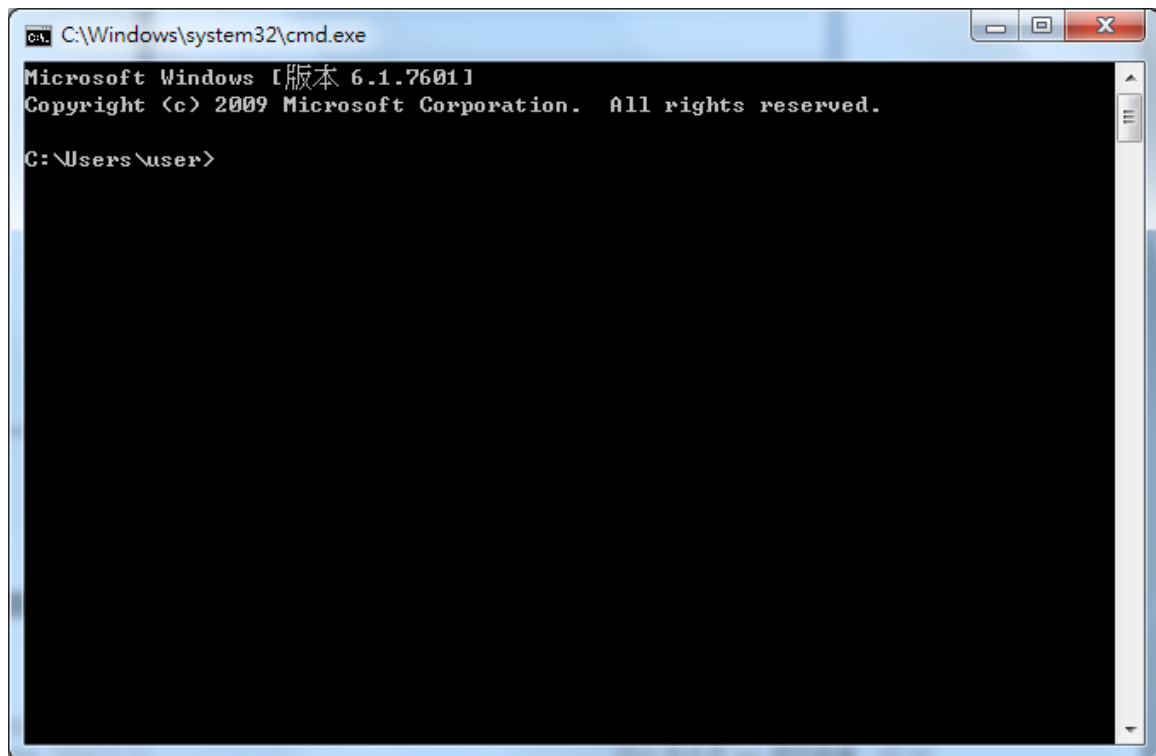




2.1.2 用”cmd”打開”命令提示字元視窗”，預設在”C:\Users\xxx>”，(xxx 為登入者名稱)，再下指令，

(1). 請按” (視窗鍵)” + “R”，出現”執行”視窗，輸入”cmd”按確定鈕。





(2). 再下指令,

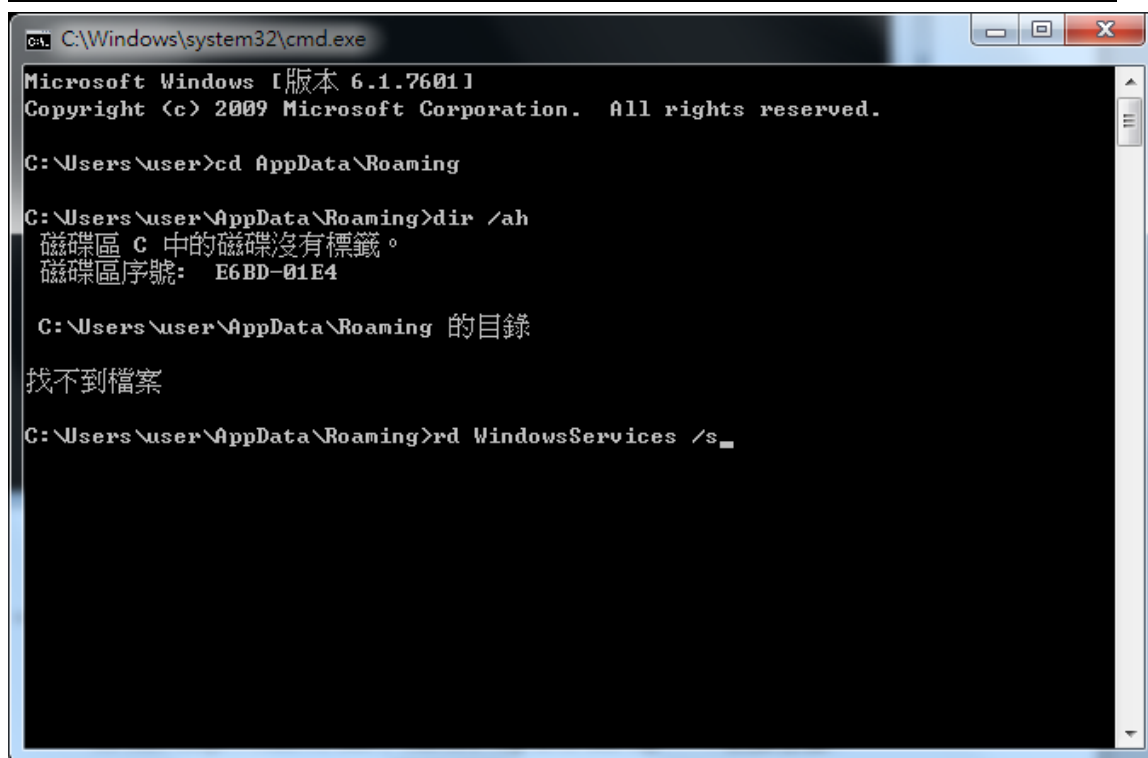
cd AppData\Roaming

dir /ah //將隱藏目錄列出, 一般正常不會有.

rd WindowsServices /s //若有 WindowsServices 目錄, 將之全刪除.

cd Microsoft\Windows\Start Menu\Programs\Startup //切換目錄.

del helper.lnk //刪除檔案.



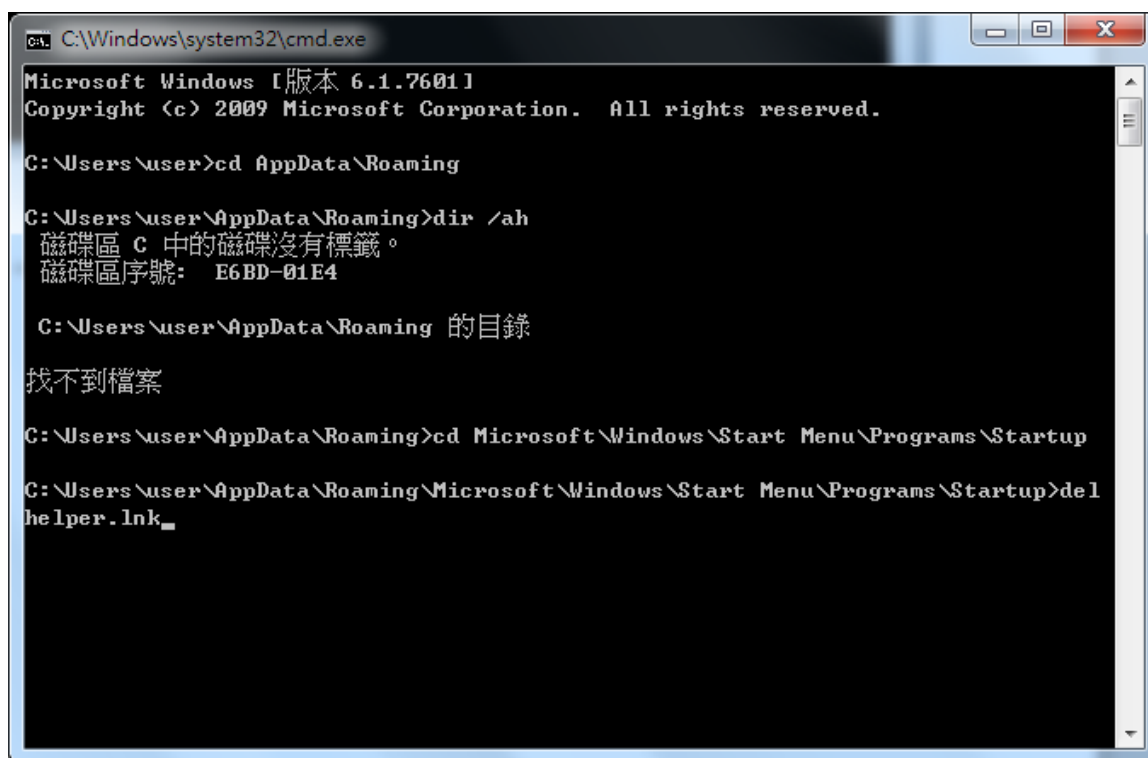
```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>cd AppData\Roaming

C:\Users\user\AppData\Roaming>dir /ah
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: E6BD-01E4

C:\Users\user\AppData\Roaming 的目錄
找不到檔案

C:\Users\user\AppData\Roaming>rd WindowsServices /s_
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>cd AppData\Roaming

C:\Users\user\AppData\Roaming>dir /ah
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: E6BD-01E4

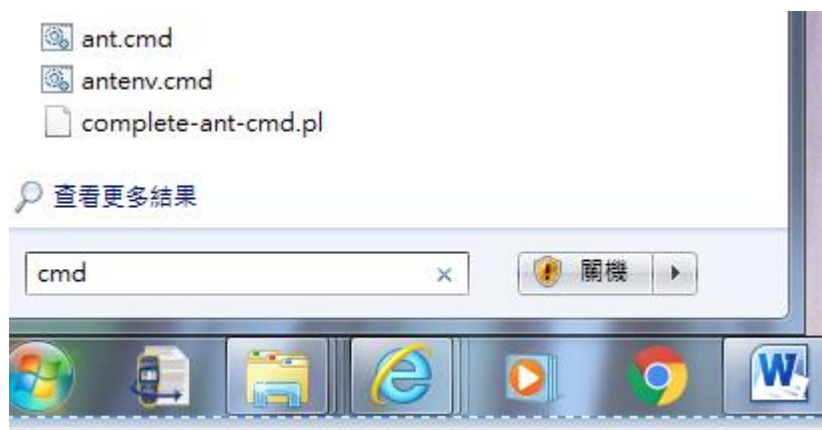
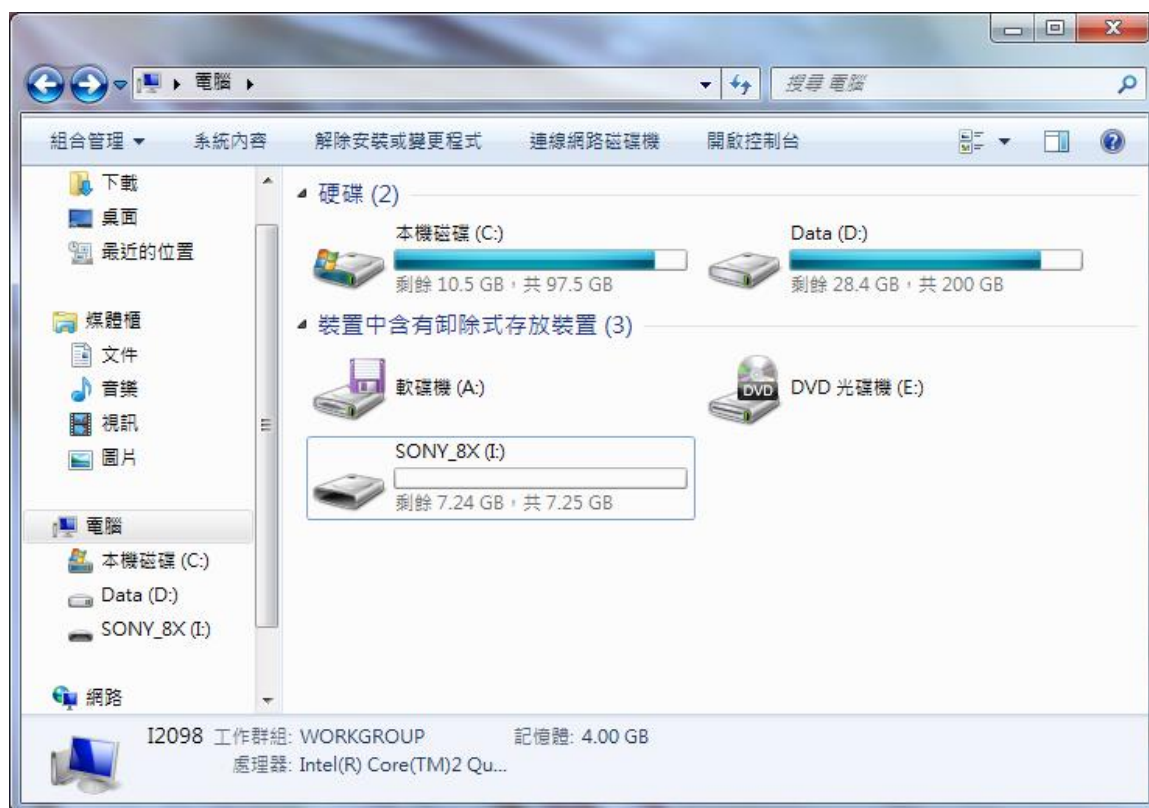
C:\Users\user\AppData\Roaming 的目錄
找不到檔案

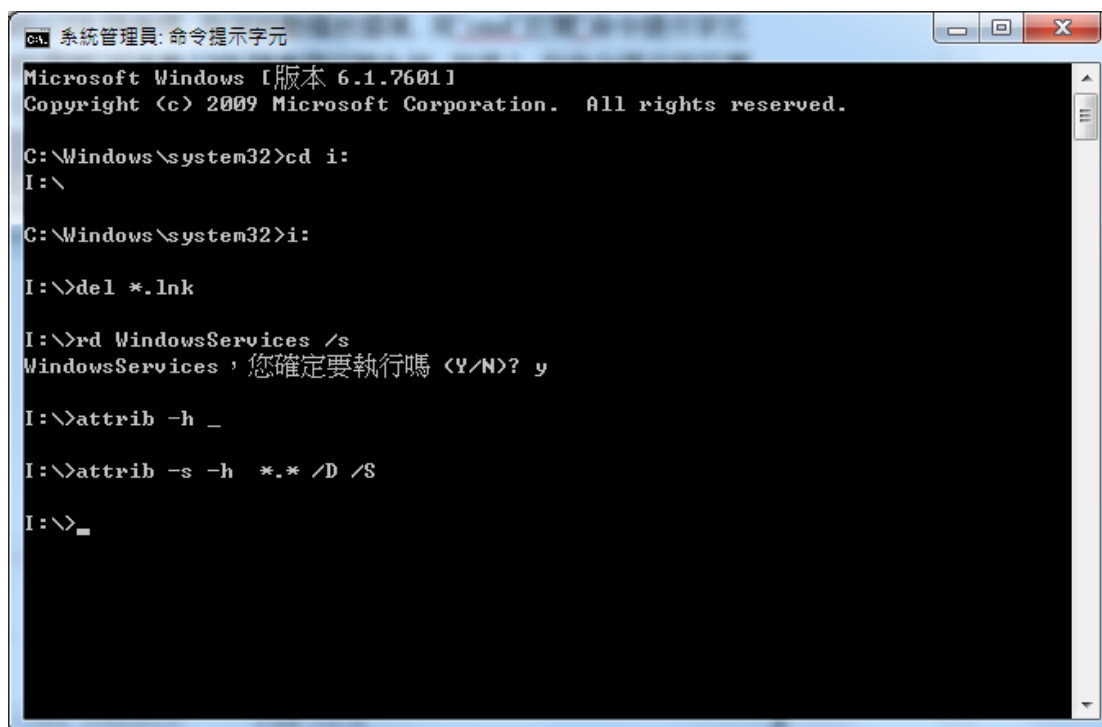
C:\Users\user\AppData\Roaming>cd Microsoft\Windows\Start Menu\Programs\Startup
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup>del
helper.lnk_
```

(3). 重新開機，回到 2.1.1，再看是否有 WScript.exe，若沒有才確認主機沒有該病毒，才可至 2.2 步驟，對 USB 隨身碟消毒。

2.2 對 USB 隨身碟消毒, (注意: 必須完成 2.1 步驟, 才能進行 2.2 步驟),

2.2.1 插入中毒的 USB 隨身碟，取消自動播放選項，用”cmd”打開”命令提示字元視窗”，打開”我的電腦”可查看 USB 隨身碟代號為何，如是 I，在命令提示字元視窗，下指令 I:，切換至 USB 隨身碟的根目錄。





(1). 再下指令,

`del xxxx.lnk` //刪除.lnk 檔, xxxx 有可能是隨身碟品牌名稱, 如.transcend.

或

`del *.lnk` //刪除全部.lnk 捷徑檔,

`rd WindowsServices /s` //隱藏檔 WindowsServices 目錄(含)檔案全刪除.

`attrib -h _` //將隱藏”_”目錄恢復顯示(內含原始文件).

或

`attrib -s -h *.* /D /S` //將被隱藏的檔案及資料夾恢復顯示

2.2.2 用檔案總管, 開啟”_”目錄, 將原始文件全選剪下, 貼回至隨身碟根目錄, 再將”_”目錄刪除(請確認是空的), 即完成清毒.

2.2.3 將隨身碟根退出主機, 再接回主機, 若發現又只變成一個.lnk 捷徑檔, 表示步驟 2.1 的主機清毒沒做好, 請再回到步驟 2.1 做起.