移動式媒體

前言：

針對當下所有人在日常工作上的習慣，時常會交換 USB Disk，也因為如此，相關的惡意程式就可以利用這一習慣點，再加上 USB 上的 Autorun（自動執行）功能，進一步植入所謂的 USB Worm。

該 USB Worm 可透過 USB 等可攜式裝置進行散播，受感染的電腦將在各磁碟機中產生 autorun.inf 檔案，當使用者在磁碟機的圖示上點兩下，便會執行 autorun.inf 與夾帶的病毒檔案，當下，該台電腦就算是淪陷了。

倘若新的且乾淨的 USB 裝置在受感染的電腦上使用後，便會將病毒檔案與 autorun.inf 複製到該乾淨的 USB 裝置內，當該裝置插入其他電腦使用時，因為自動播放功能會自動執行 autorun.inf，病毒便可再次感染其他電腦，也因為如此擴散再擴散，將有可能一發不可收拾。

隨身硬碟是很好用的儲存裝置，體積越做越小，容量越做越大，要讓各位不要用是根本不可能的且確實很不方便，所以相對的，只要做些防護措施當然也是可以快快樂樂的用。

如何得知被感染：

1. 無法開啟系統中的磁碟機，連點兩下磁碟機代號，會沒有回應或出現錯誤訊息。

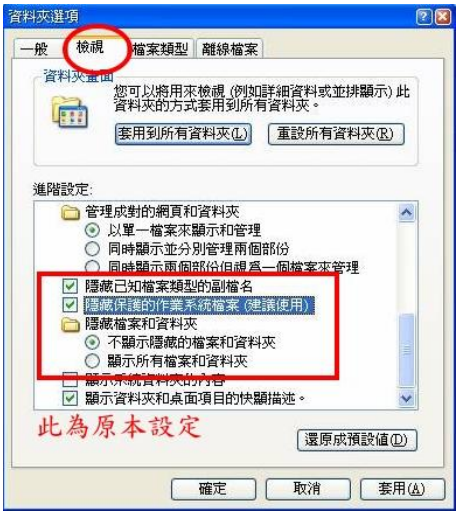
唯一開啟方式只有利用「檔案總管」，對磁碟機按右鍵。

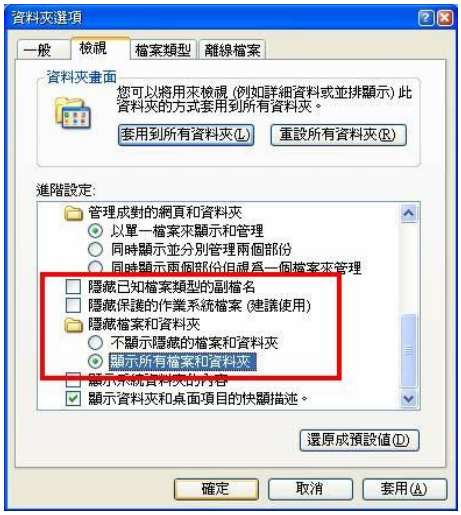
2. 如發生上述異常時，很有可能病毒確實被防毒軟體阻擋並移除，但病毒已啟動 autorun.inf 於磁碟上，造成系統無法正確讀取磁碟區域內容。此外如果有中毒防毒軟體又沒辦法有此預防，那就表示防毒軟體沒有定期更新。

中毒了該怎麼解決？

1. 設定成可以看到隱藏檔

打開「我的電腦」後,從上方工具列中的「工具」->「資料夾選項」打開資料夾選項視窗,從「檢視」的頁籤,下方找到這幾個項目: 隱藏已知檔案類型的副檔名,隱藏保護作業系統檔案,隱藏檔案和資料夾.





2. 利用「檔案總管」開啟行動硬碟，再把 autorun.inf 移除，就暫時解除危機。

預防方法：

方法一：從行動硬碟本身下手，在行動硬碟中一樣建立一個 autorun.inf 的檔案，並且把這檔案設定成唯讀（只可以讀，不能寫）。
一般未自行建立該執行檔的情形下，當別人的電腦已經中毒了，您把隨身碟借他，在插入時也順便把 autorun.inf 一併傳給你，當你已經先建立此檔並且唯讀，真正的的病毒 autorun.inf 就寫不進來啦！當然你的行動硬碟也不會變成「帶原者」。

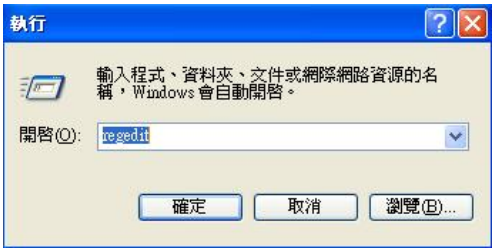
在行動硬碟建立 autorun.inf 這個檔後，

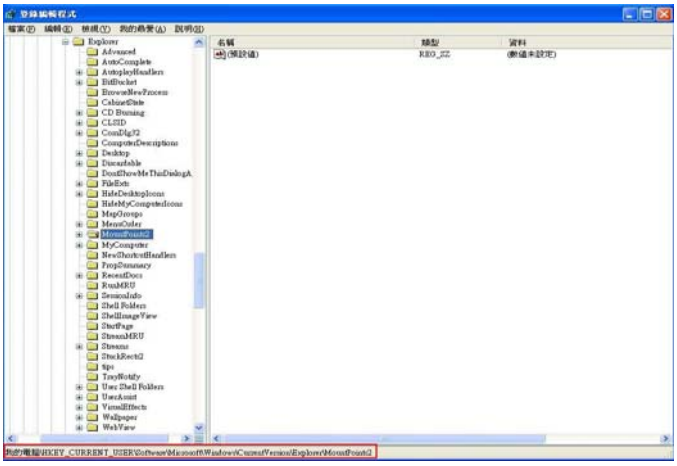
對資料夾按右鍵->內容，把唯讀選項打勾

當複製同樣檔名的檔案在這行動硬碟內，就會出現錯誤訊息，這樣真正的病毒 autorun.inf 就寫不進來了。這方法保護了別人，但是要怎麼保護自己？

方法二：把行動裝置的自動執行給停用。這個是最好用的方法，但是這必須改機碼，比較不建議改機碼，因為機碼是作業系統核心的部份，如果一不小心改錯了就可能導致無法開機，最終下場就是重灌嘍。

開始 -> 執行 後輸入 regedit。

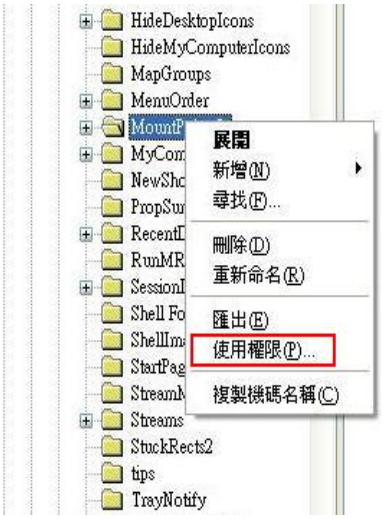




紅色框就是修改路徑的地方。

HKEY_CURRENT_USER\Software\microsoft\Windows\CurrentVersion\Explorer\Mountpoints2

MountPoints2 按下滑鼠右鍵，選擇 使用權限



把常用的幾個帳號的權限完全控制和讀取這兩個項目（最重要的帳號 Administrators 這是一定要），都在拒絕那給打勾，在按下套用及確定，即可將任何的 USB 裝置自動執行 autorun.inf 都禁止，利用 autorun.inf 來執行的隨身碟病毒就會失效。

方案三：利用一些小工具來幫忙做檢測

WowUSBVirusKiller 是由中央研究院資訊科學所自由軟體鑄造場所推出的一款「專門」用來防護 USB 病毒及偵測和清除的保護軟體，這支程式比較適合一般的使用者，或著不想麻煩的電腦用戶，所有的偵測及防護都會自動執行，且發現病毒會自動刪除，並不會知會使用者，使用就不需判斷該如何處理狀況。這只有防護 USB 的喔，不是說用了這個防毒軟體就不用裝，要注意！

以上的方法都可以針對 USB 做防護，當然的，最重要的也是作業系統本身要定期的更新，防毒軟體要定期掃毒更新，這樣才會有一個安全的作業環境。

多一點確認，少一分損失

資料提供：國立嘉義大學電算中心