ＵＳＢ隨身碟病毒防制方法

壹、 什麼是隨身碟病毒？

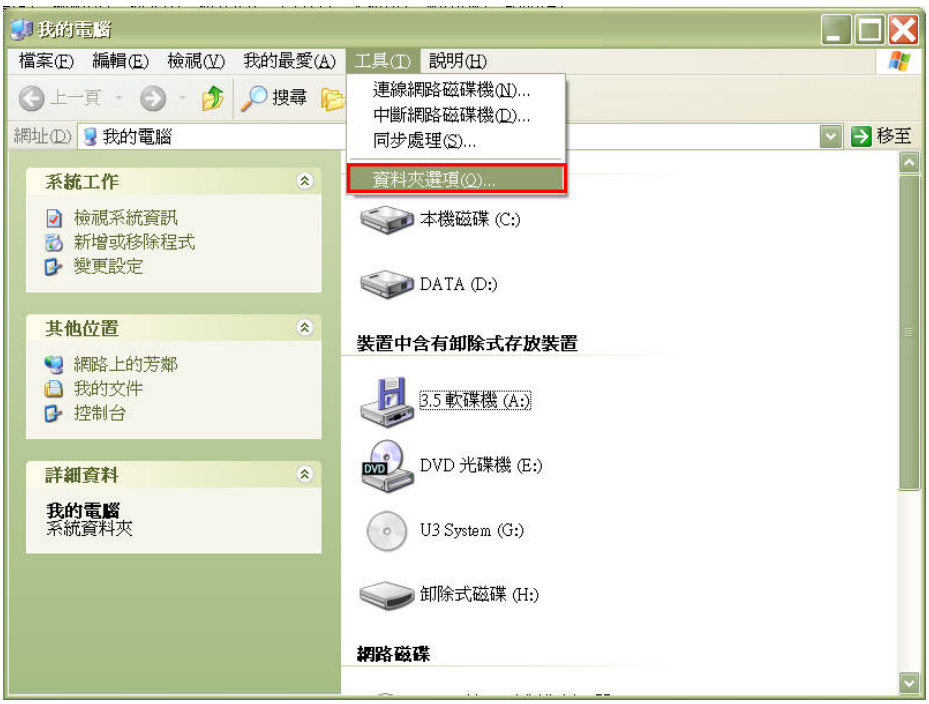
USB 隨身碟病毒又稱 autorun 病毒。預設當電腦偵測到 USB 裝置時，Windows 系統會自動尋找並執行 autorun.inf，進而執行其他應用程式。USB 病毒主要是利用 autorun.inf 將病毒植入電腦主機，使對方的硬碟分享出來或安裝惡意程式，或反向從遭感染的主機把病毒散播到各種 USB 介面的儲存裝置中。就是因爲具有這種雙向傳遞的方式，病毒才能在電腦及 USB 儲存裝置中不斷擴散，而 autorun.inf 就是最主要的媒介。

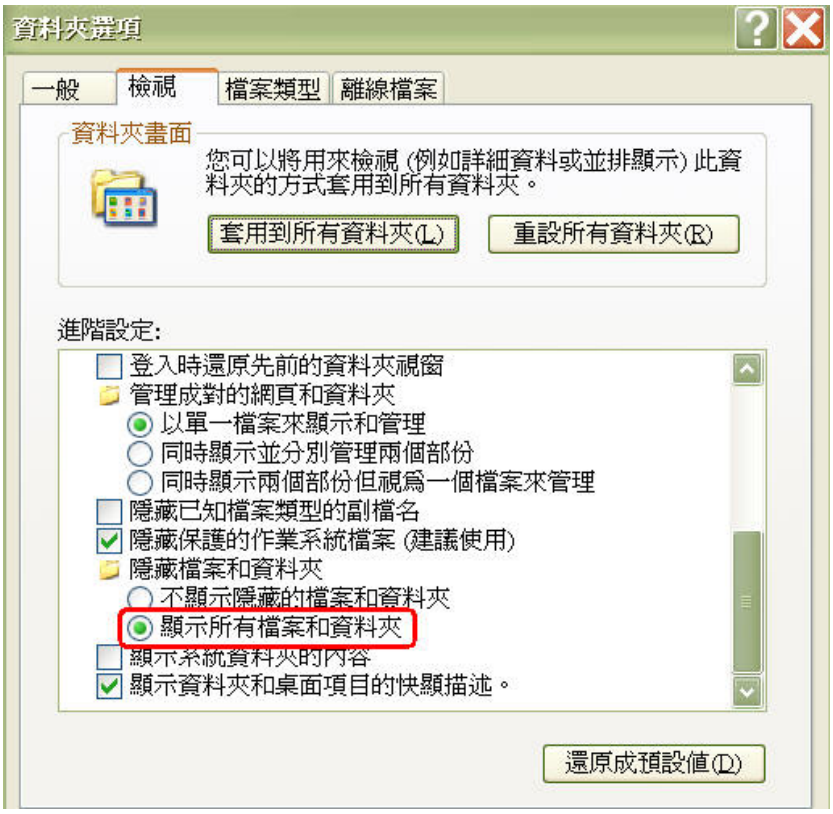
autorun.inf 這個純文字檔是讓電腦能自動播放程式的參考依據，當初它的目的是，使用者執行可移除式媒體（包括光碟、隨身碟及硬碟等）時，簡化需自行進入媒介中，手動點選程式的麻煩。autorun.inf 本身並不是惡意程式，但惡意程式可以利用 autorun.inf 的內容，自動且隱密地進入電腦主機中，而且由於 Windows 作業系統在預設情況下，允許自動執行 autorun.inf，也讓病毒感染速度更快。

隨著 USB 隨身碟，外接式硬碟，存儲卡等移動儲存裝置的普及，USB 隨身碟病毒也隨之氾濫起來。近年來 USB 磁碟已成爲病毒和惡意木馬程式傳播的主要途徑。

貳、 中毒後主要現象：

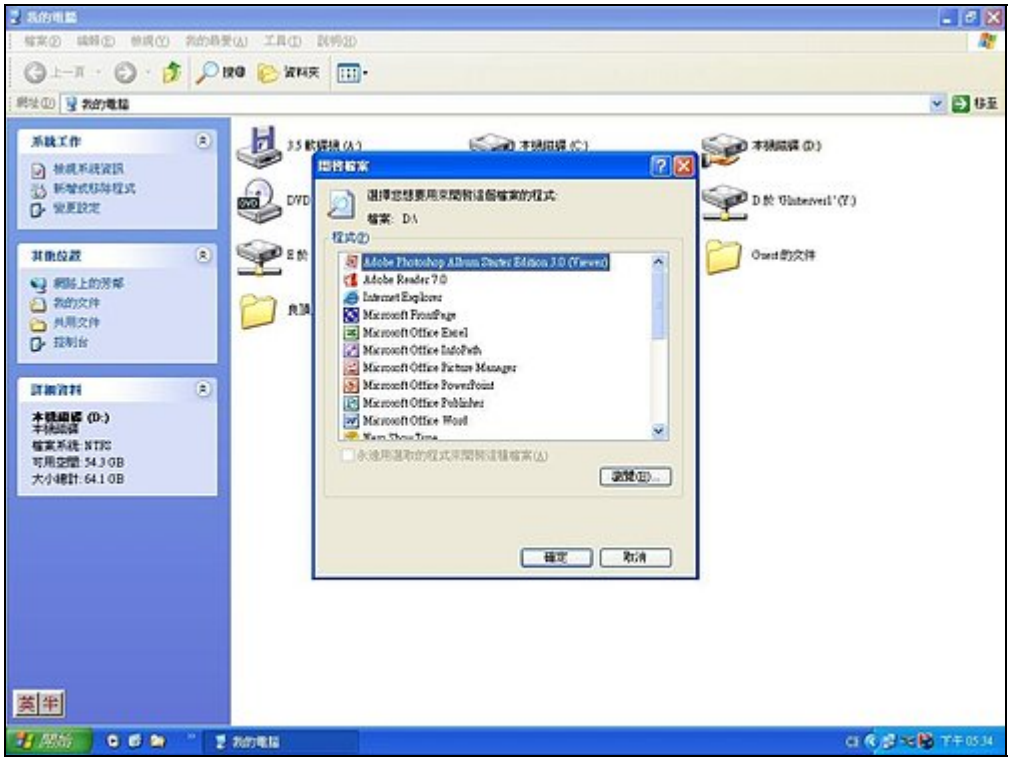
一、無法於「資料夾選項中」設定『顯示所有的檔案和資料夾』。操作如下：開啓我的電腦→工具→資料夾選項→檢視→顯示所有檔案和資料夾。





若選了「顯示所有檔案和資料夾」，按確定後再回來看一次，如果它又自己跳回來「不顯示隱藏的檔案和資料夾」，那就是中毒了

二、進去桌面上我的電腦想要打開硬碟 如 c,d,e 槽，卻出現「選擇程式來開啓檔案」(如下圖)，或是某磁碟打不開，則表示有中毒跡象



三、其他可能中毒跡象：

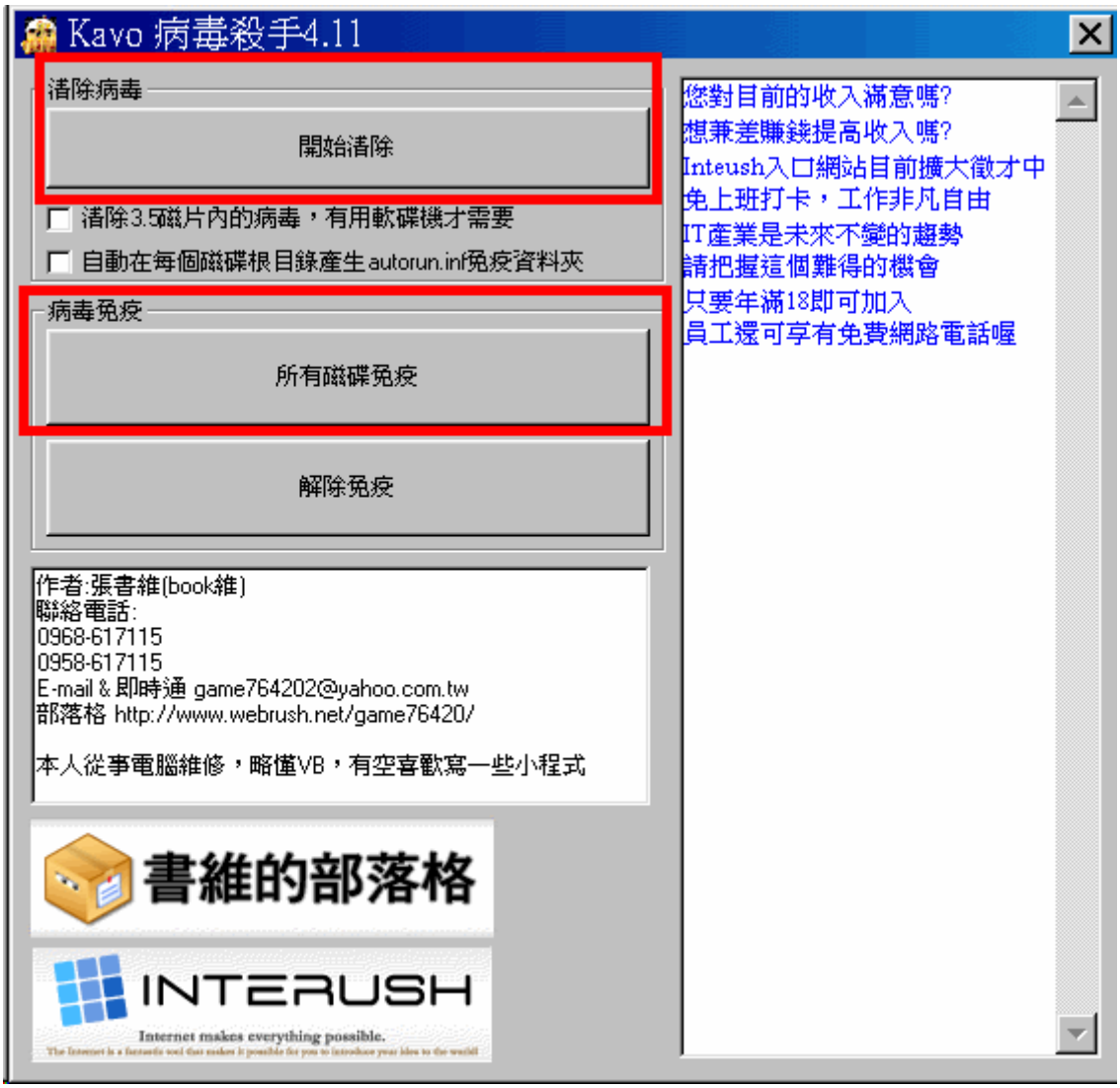
（一）即時通登入後會自動關閉。
（二）防毒軟體會被停用。
（三）網路驅動程式發生錯誤 導致無法連線。

參、 介紹 KAVO 病毒（著名 USB 病毒）清除方式

一、病毒運作模式：利用 inetsrv.exe 掩護位於隨身碟的 driveinfo.exe 、driveinfo.sdc、voinfo.dll、 autorun.inf，這些檔案被系統保護住，需要將「工具」裡的「資料夾選項」的「檢視」，將裡面的「隱藏保護的作業系統檔案」打勾去除才能看到這些檔。若中了 KAVO 病毒就會出現要打開硬碟 如 c,d,e 槽，卻出現「選擇程式來開啓檔案」的現象。

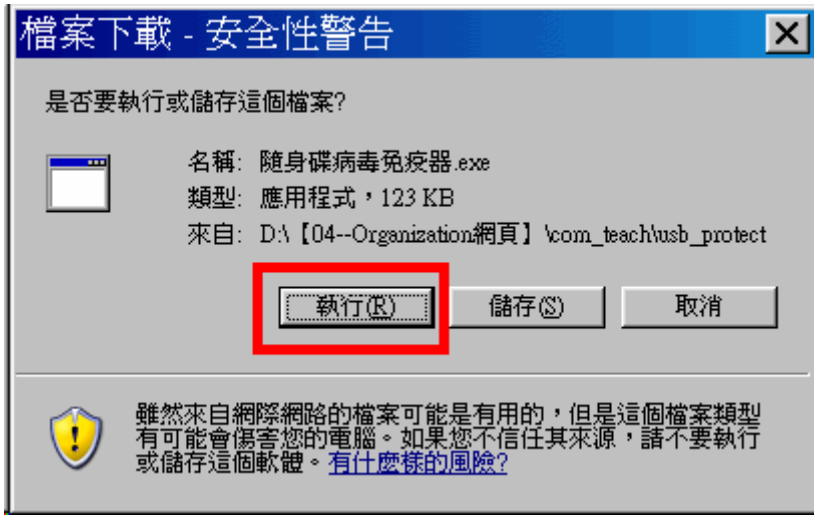
二、解毒與防疫：

（一）已中毒者，請下載並執行『kavo_killer』！檔案連結網址如下：
http://msa.yses.tpc.edu.tw/~organization/com_teach/usb_protect/kavo_killer.exe

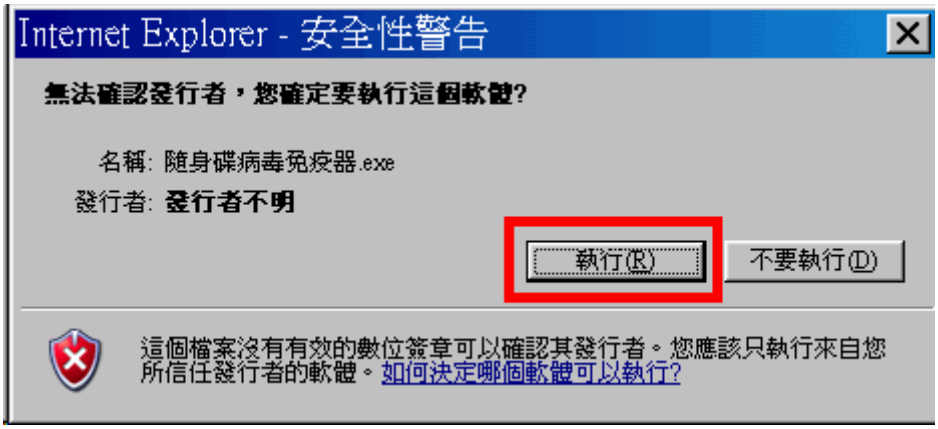


（二）解完毒或尚未中毒者，請下載並執行『隨身碟病毒免疫器』！預防日後中 USB 病毒。檔案連結網址如下：

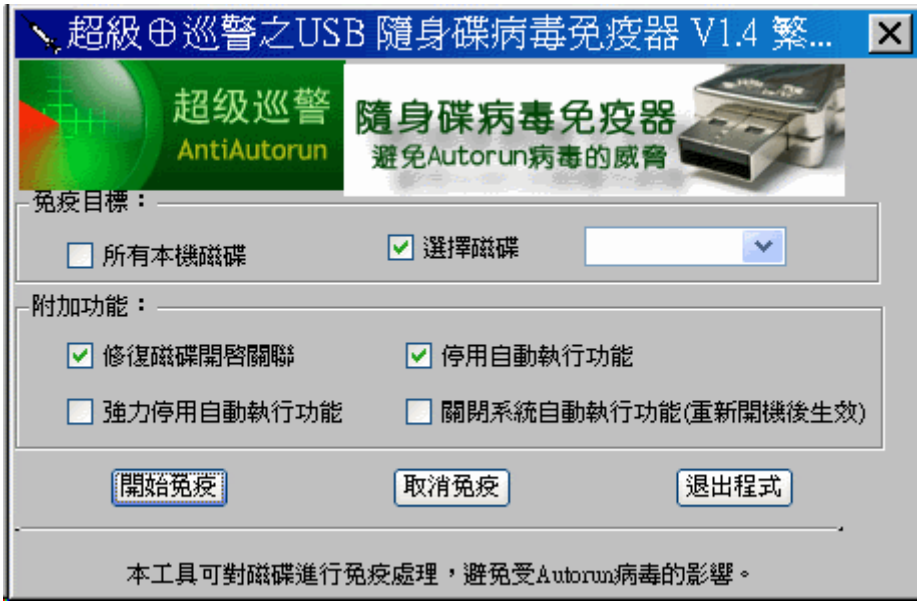
http://msa.yses.tpc.edu.tw/~organization/com_teach/usb_protect/usb_protect.exe



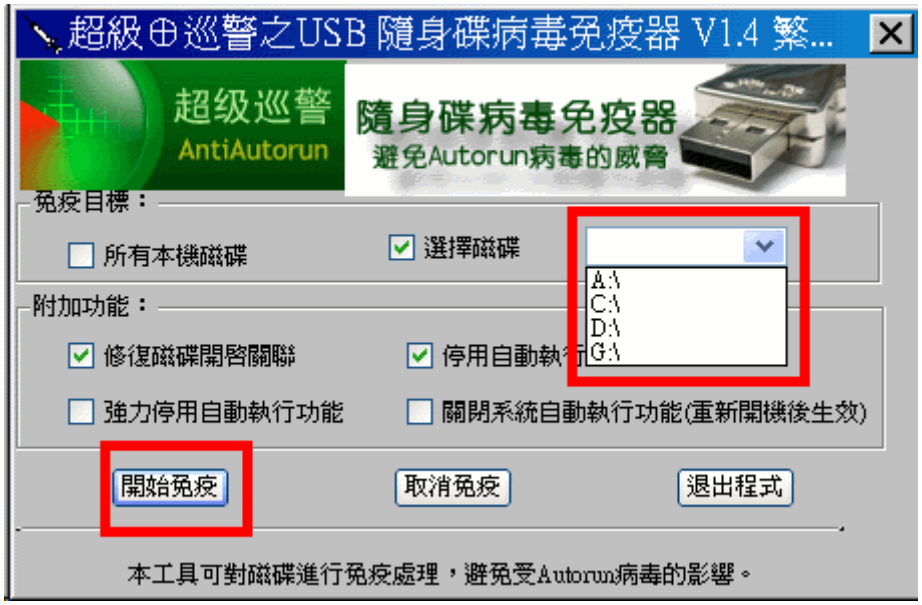
（三）請繼續選擇『執行』！



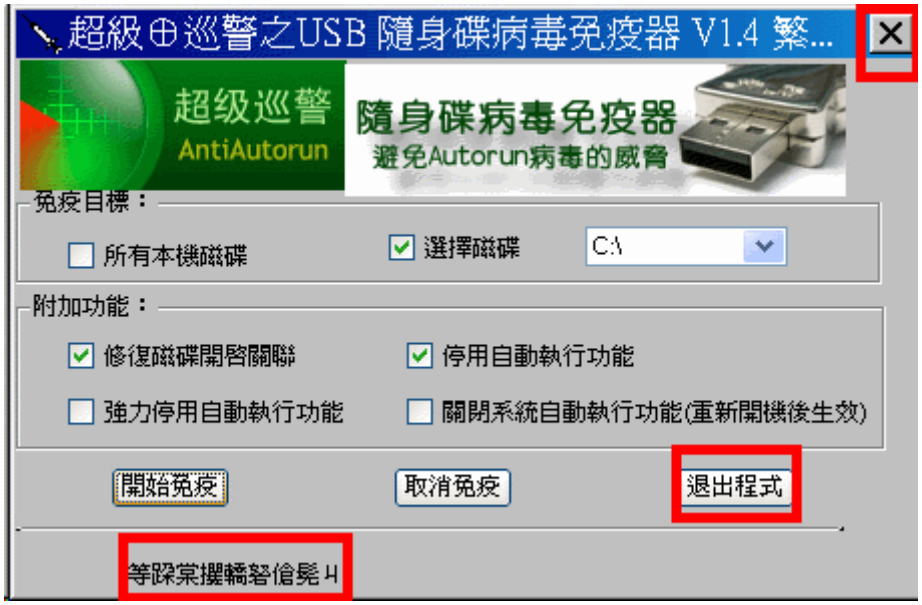
（四）接著會出現如下圖之畫面：



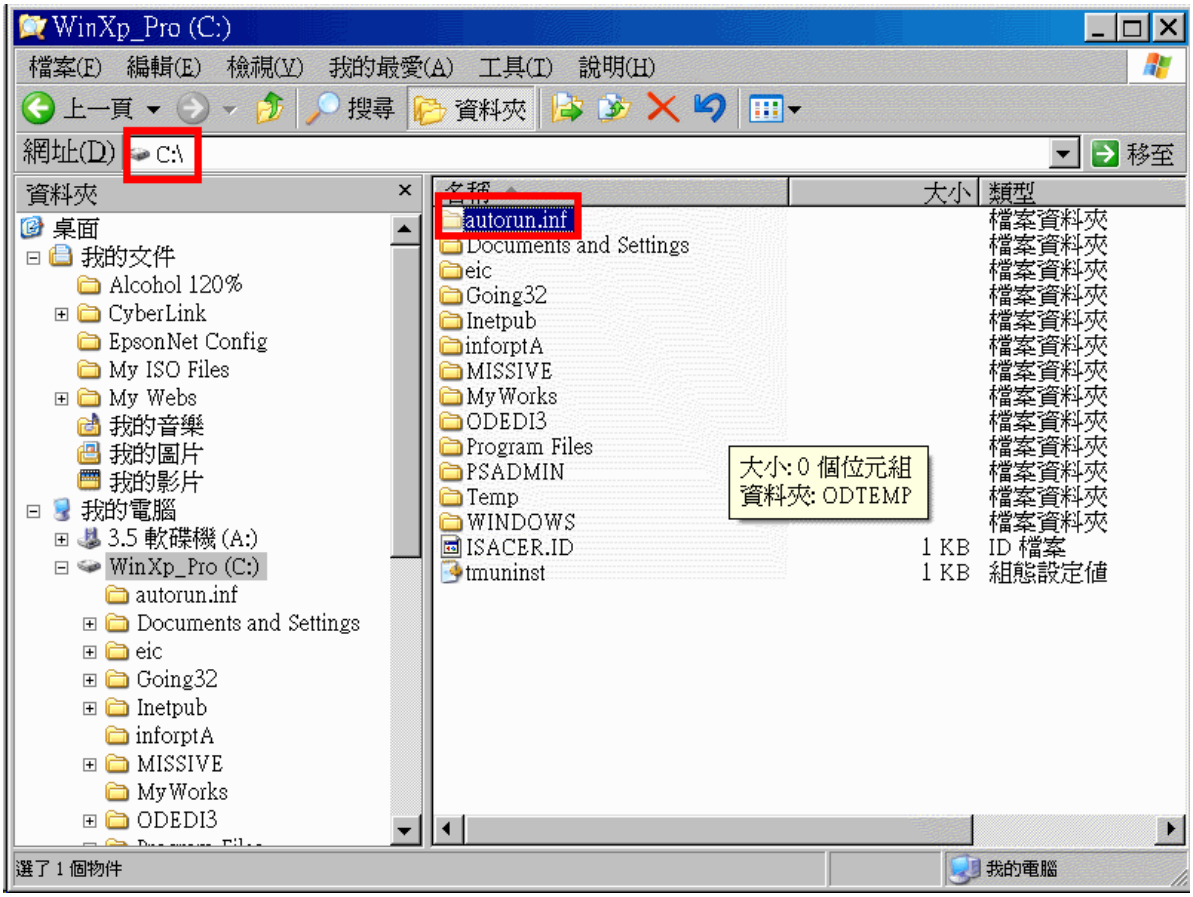
（五）請 選擇隨身碟所代表之磁碟機代號，然後請按 『開始免疫』！



（六）下方出現亂碼字（因爲此版本是翻譯版，有些地方沒翻譯好），按『退出程式』或『關閉』即可！



（七）檢查您所免疫的磁碟裡，就會出現一個『autorun.inf』的資料夾，就可以開始免疫囉！【若看不見，請檢查該部電腦是否能觀看隱藏檔？若不行，請開啓權限後再觀看之！】，『隨身碟病毒免疫器』幫您建立一個『autorun.inf』的空資料夾，主要目的在防止病毒藉由『autorun.inf』載入，減少遭植入病毒的機會。



（八）由於病毒也有可能感染其他磁碟，建議您其他磁碟機（光碟機除外）也一併免疫比較保險喔！

肆、 其他清除 USB 病毒的方式

除了安裝一般的防毒軟體（如賽門鐵克或小紅傘），網路上也有一些專門清除 USB 病毒的工具，常見的有 USB Cleaner、USB Protector、、、等。USB Cleaner 使用說明網址：http://briian.com/?p=5155。USB Protector 使用說明網址：http://www.openfoundry.org/index.php?option=com_content&Itemid=144&id=1462&lang=en&task=view。PS：網路上清除 USB 病毒的工具很多，請選擇較著名或較多人使用的工具，避免使用不明程式以免反造成中毒。

【參考及引用資料來源】

1、http://msa.yses.tpc.edu.tw/~organization/com_teach/usb_protect/index.htm

2、http://tw.myblog.yahoo.com/jw!CUdqzyaREw8BmvXftg--/article?mid=56

（本文由行政院主計處電子處理資料中心設計員邱弘朝 提供）