電腦故障排除 -電腦安全防護

電腦故障排除 -電腦安全防護

一、認識隨身碟病毒

二、如何防護電腦避免中毒(正確使用隨身碟)

三、如何清除電腦及隨身碟病毒
A：手動清除
B：efix介紹及使用

四、建置一個病毒無法入侵之隨身碟

認識隨身碟病毒

第一代

Kavo、TAVO、TASO、KASO等

第二代

資料夾**.exe**病毒

第三代

msbackup.exe

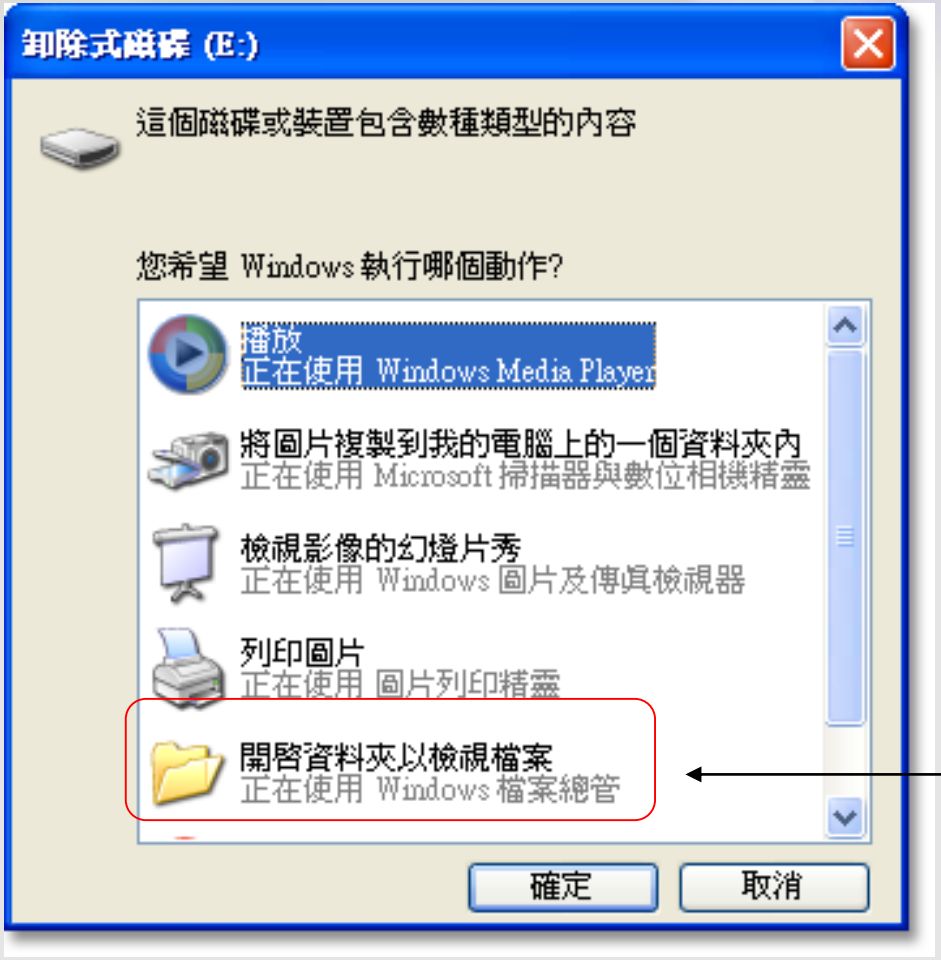
Kavo病毒

一、利用autorun.inf執行Ntdelect.com 程式。

二、Ntdelect.com複製Kavo.exe到
C:\windows\system32底下

三、Kavo.exe是主要病毒檔，當此程式執行時會在各磁碟機建立ntdelect.com和autorun.inf，並不斷耗損電腦記憶體，導致電腦運行很慢，有時甚至會使電腦當機。

Kavo病毒



Autornu.inf檔案內容

```
[AutoRun]
open=ntdelect.com
;shell\open=Open(&O)
shell\open\Command=ntdelect.com
shell\open\Default=1
;shell\explore=Manager(&X)
shell\explore\Command=ntdelect.com
```

點選這個按確定即會執行autorun.inf檔

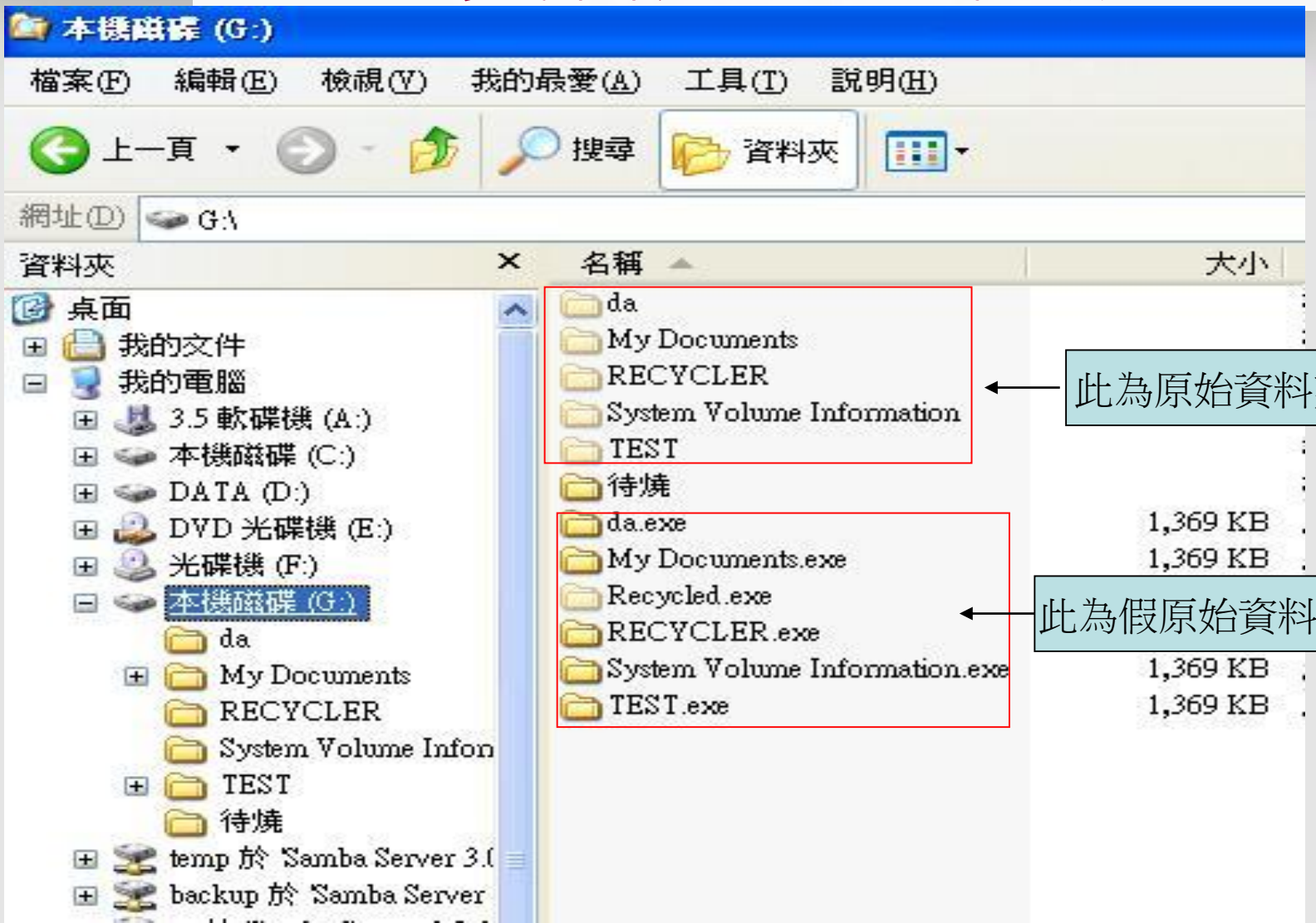
資料夾.exe病毒

一、將隨身碟中原本的資料夾隱藏

二、新增和原本資料夾名稱的.exe檔案，並將圖示改成資料夾。

三、新增autorun.inf檔案，隨身碟插入電腦後，會自動執行蠕蟲。

資料夾.exe病毒


本機磁碟 (G:)
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
資料夾
網址(D) G:\
資料夾
名稱
大小
桌面
我的文件
我的電腦
3.5 軟碟機 (A:)
本機磁碟 (C:)
DATA (D:)
DVD 光碟機 (E:)
光碟機 (F:)
本機磁碟 (G:)
da
My Documents
RECYCLER
System Volume Infon
TEST
待燒
temp 於 'Samba Server 3.(
backup 於 'Samba Server
da
My Documents
RECYCLER
System Volume Information
TEST
待燒
da.exe 1,369 KB
My Documents.exe 1,369 KB
Recycled.exe
RECYCLER.exe
System Volume Information.exe 1,369 KB
TEST.exe 1,369 KB
此為原始資料夾被隱藏
此為假原始資料夾病毒檔

Msbackup.exe

一、利用autorun.inf執行msbackup.exe。

二、複制msbackup.exe到各磁碟機裡。

三、在啟動區建立啟動

四、主要影響

C:\WINDOWS\system32\calc.exe(小算盤)

C:\WINDOWS\system32\sndvol32.exe(音量)

如何防護電腦避免中毒

一、防毒軟體版本的更新(NOD4.2)

請至電算中心資訊安全防護網站下載新版防毒軟體

http://203.64.35.39

二、手動檢查

請參考下列網址

http://203.64.35.39/files/kavo/usb.htm

如何清除電腦及隨身碟病毒

一、手動移除檢查

msconfig指令(xp、win7適用)

二、**EFIX軟體介紹**

請參考下列網址

http://reinfors.blogspot.com/

建置一個病毒無法入侵之隨身碟

請參考下列網址

http://203.64.35.39/files/acl/index.htm

程式下載

http://203.64.35.39/files/tccn.exe

簡易說明如下：

一、先將隨身碟格式化或轉換成**NTFS**檔案格式

二、在隨身碟裡建立一個可以存放的資料夾

三、利用**cacls**將隨身碟根目錄設定為無法讀取