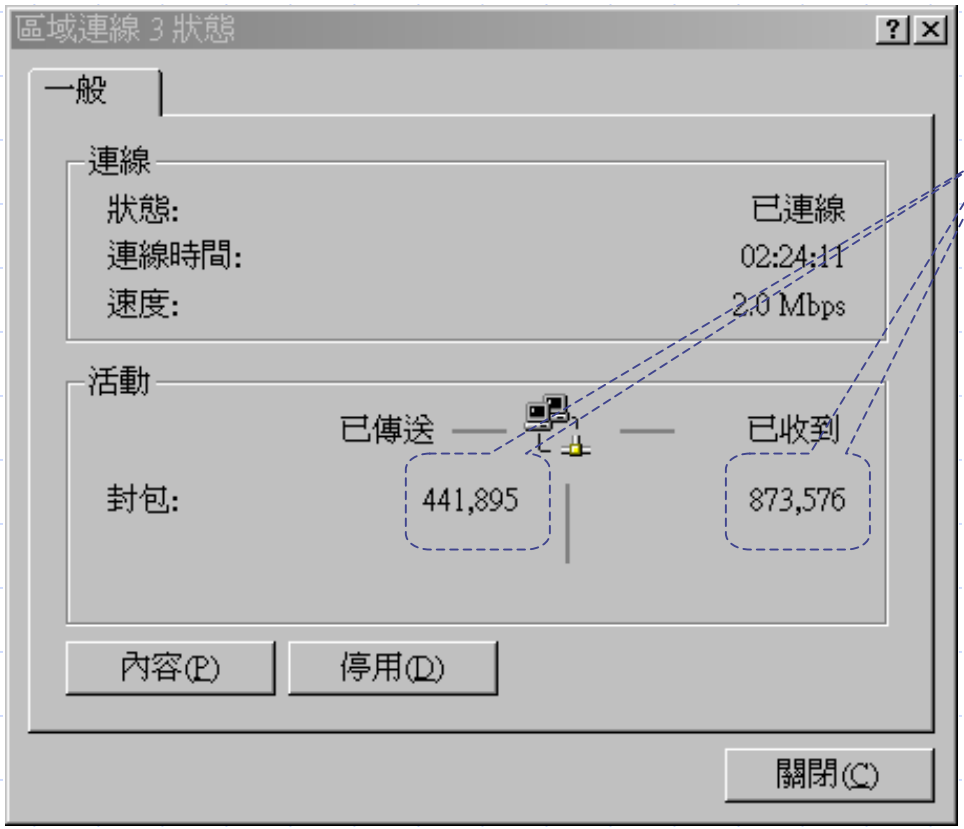
Windows系統
入侵檢測與處理

成大計網中心
楊峻榮
2004/5/20

使用時機及頻率

- 主要判斷已遭或疑似入侵（ex 系統效能不佳）之檢測及處理，針對核心項目或入侵模式
- 手動方式檢測，必須加上人為判斷（ex遭入侵或破壞之經驗累積)或和別部主機交叉比對
- 當發覺系統負載及流量異常時之手動檢測
- 固定時間約二週檢測一次
- 以Windows 2000/XP/2003 為例
- 參考防毒軟體公司網頁之[手動移除病毒程序]
- 善用登錄表編輯程式，更改登錄表前先將登錄表之該資料夾匯出,以便出狀況時匯入。但若對登錄表內容不甚了解，勿輕易嘗試。
- 屬於進階使用註明或非例行之檢測，註明＊

傳輸狀況



開啟連線狀態視窗，在沒有傳輸資料情況下，是否在傳輸大量資料。若是，可能是DOS或DDOS攻擊。

連線狀態(netstat)

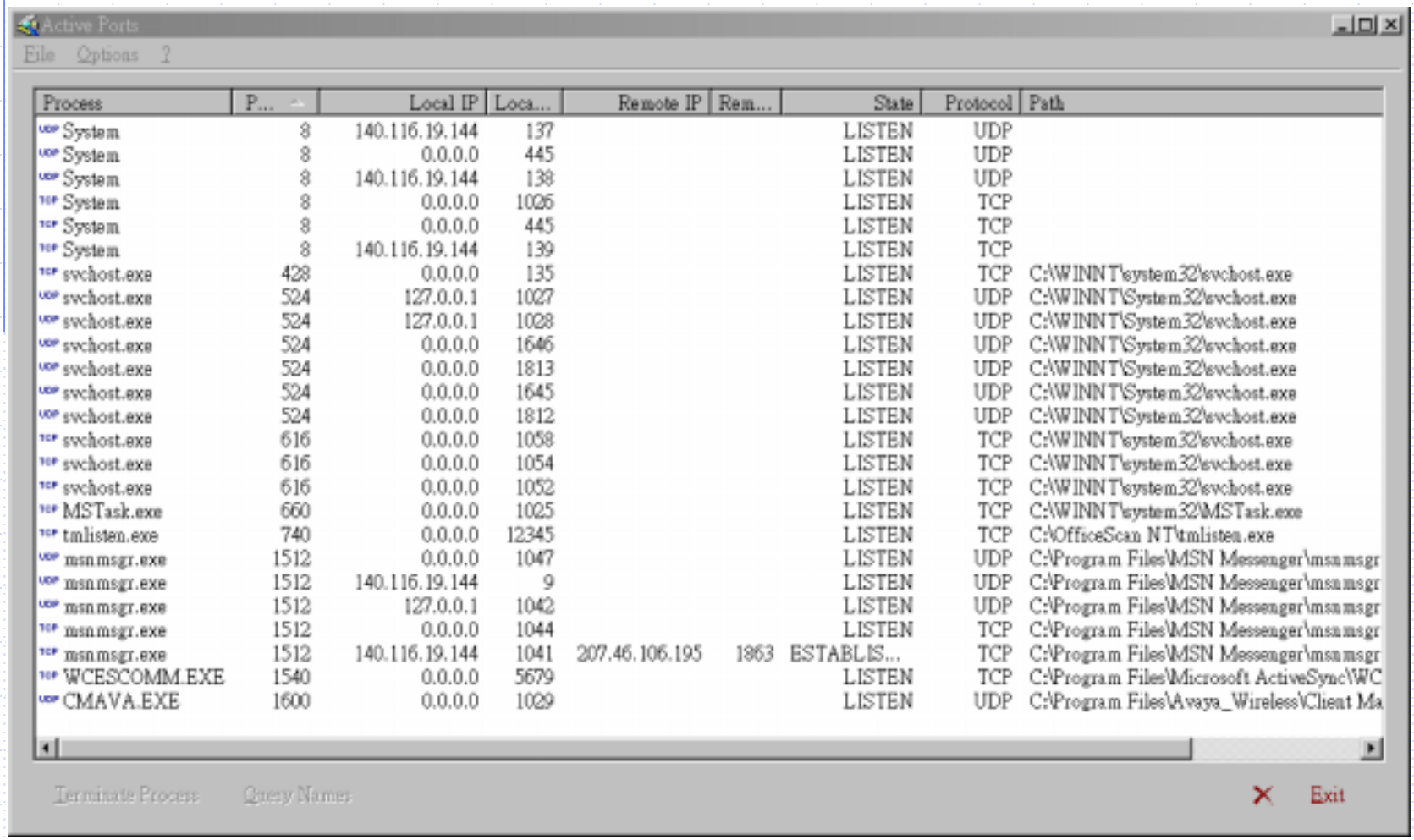
開啟　開始／程式集／附屬應用程式／命令提示字元，在該視窗下鍵入 netstat ，看看是否有不尋常之連線。

Proto	Local Address	Foreign Address	State
TCP	yang:1026	yang:20032	ESTABLISHED
TCP	yang:20032	yang:1026	ESTABLISHED
TCP	yang:3024	dec4000.cc.ncku.edu.tw:22	ESTABLISHED
TCP	yang:3613	mail.ncku.edu.tw:telnet	ESTABLISHED

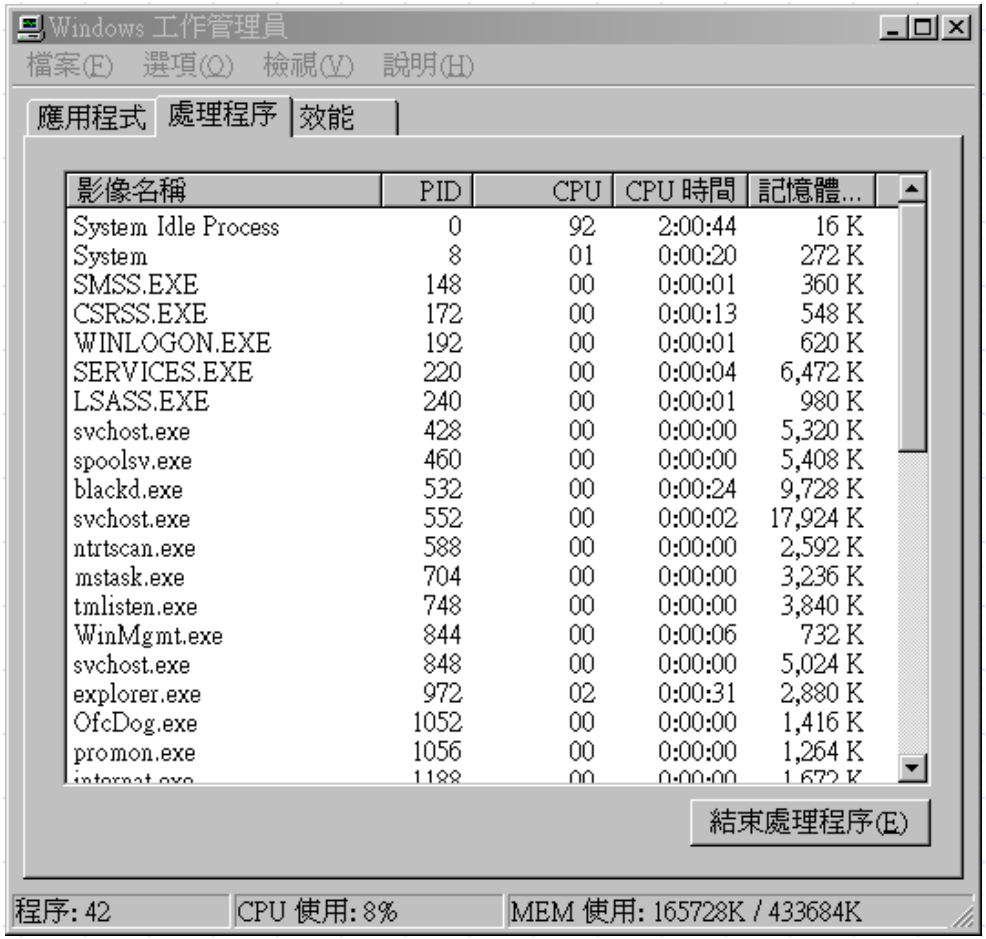
其中Froeign Address表示對方的Address及port，而State之連線狀態，如此例ESTABLISHED表示已連上。
因一般人可能很難了解Services port是代表什麼及是從本機連出或由外部連進來的，一般而言Server端port的號碼是固定的，而client端是動態的。故只要發覺Foreign Address並不是您所要連線之位置，就該注意。

連線狀態(active port)

- Freeware軟體，主要可顯示所對應之執行程式



Process(工作管理員)

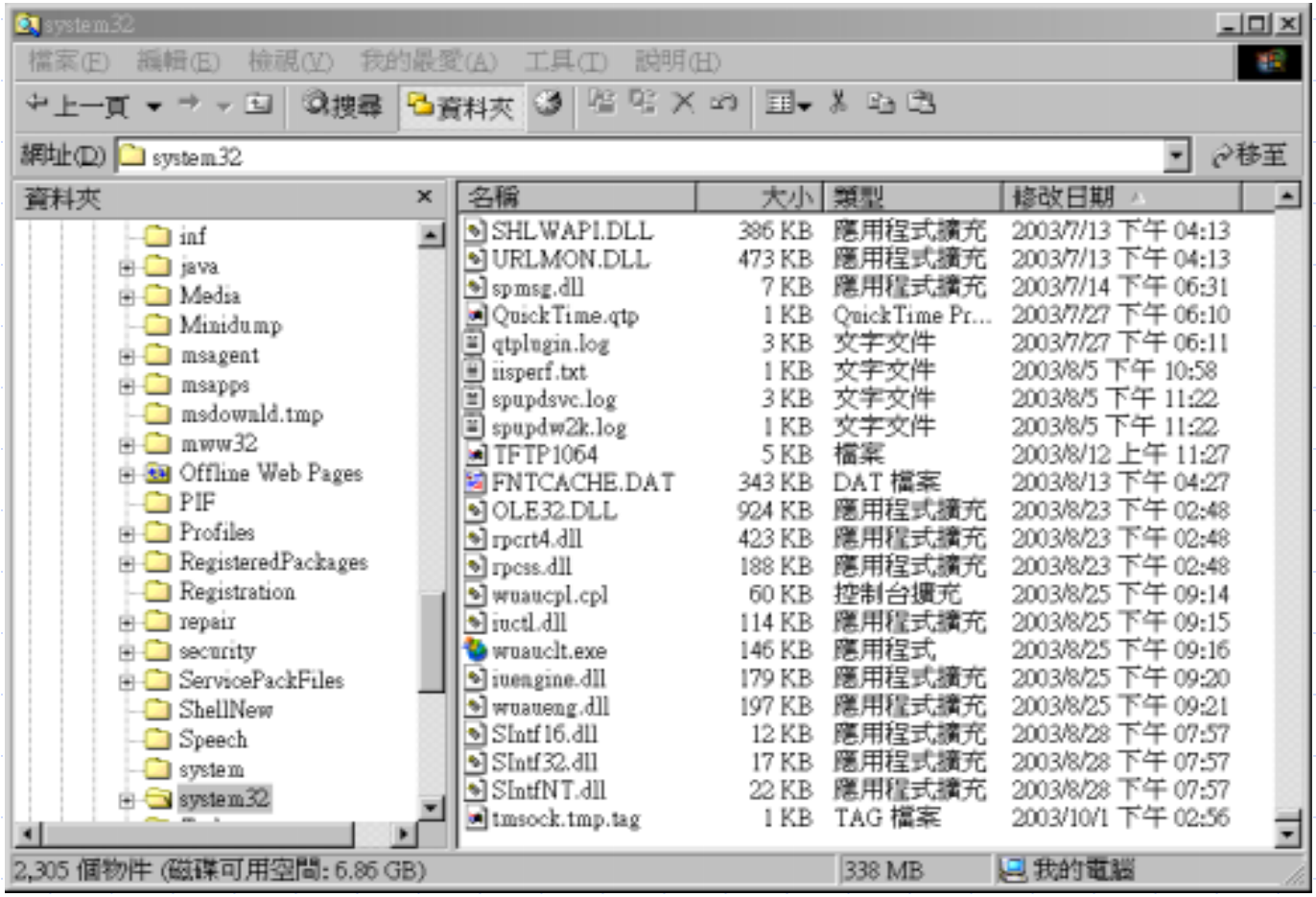


開啟工作管理員（按Ctrl+Alt+Del鍵，點選工作管理員），按下處理程序頁

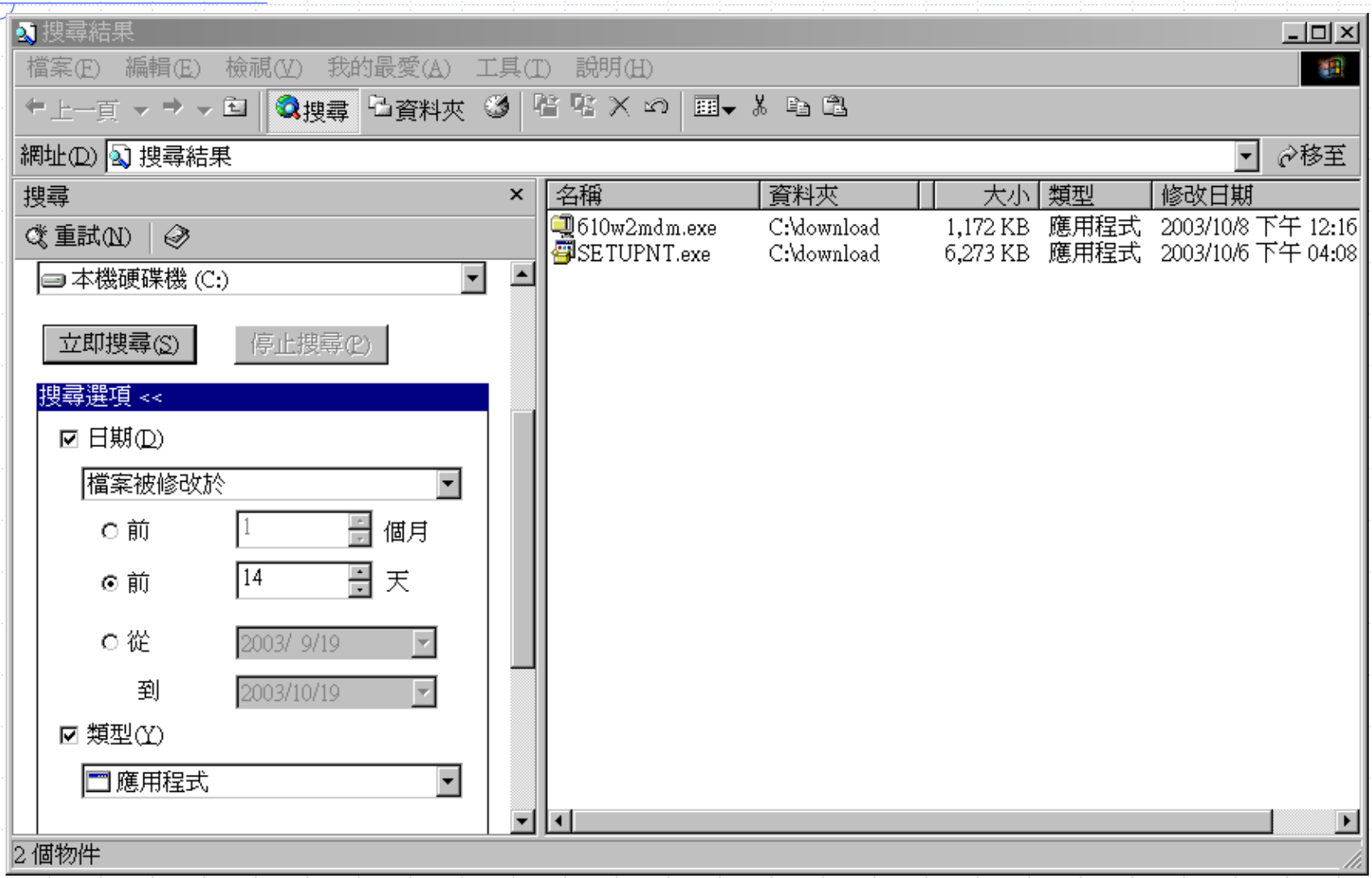
- 檢查是否有在耗用CPU但卻非自己所欲執行之程式。
- 是否有佔用大量CPU或記憶體之程式

由檔案總管檢查檔案異動日期

以「詳細資料」及「排列圖示／依日期」看最近異動之執行檔。
預設Win2000為/WINNT/system32, WinXP為/Windows/system32

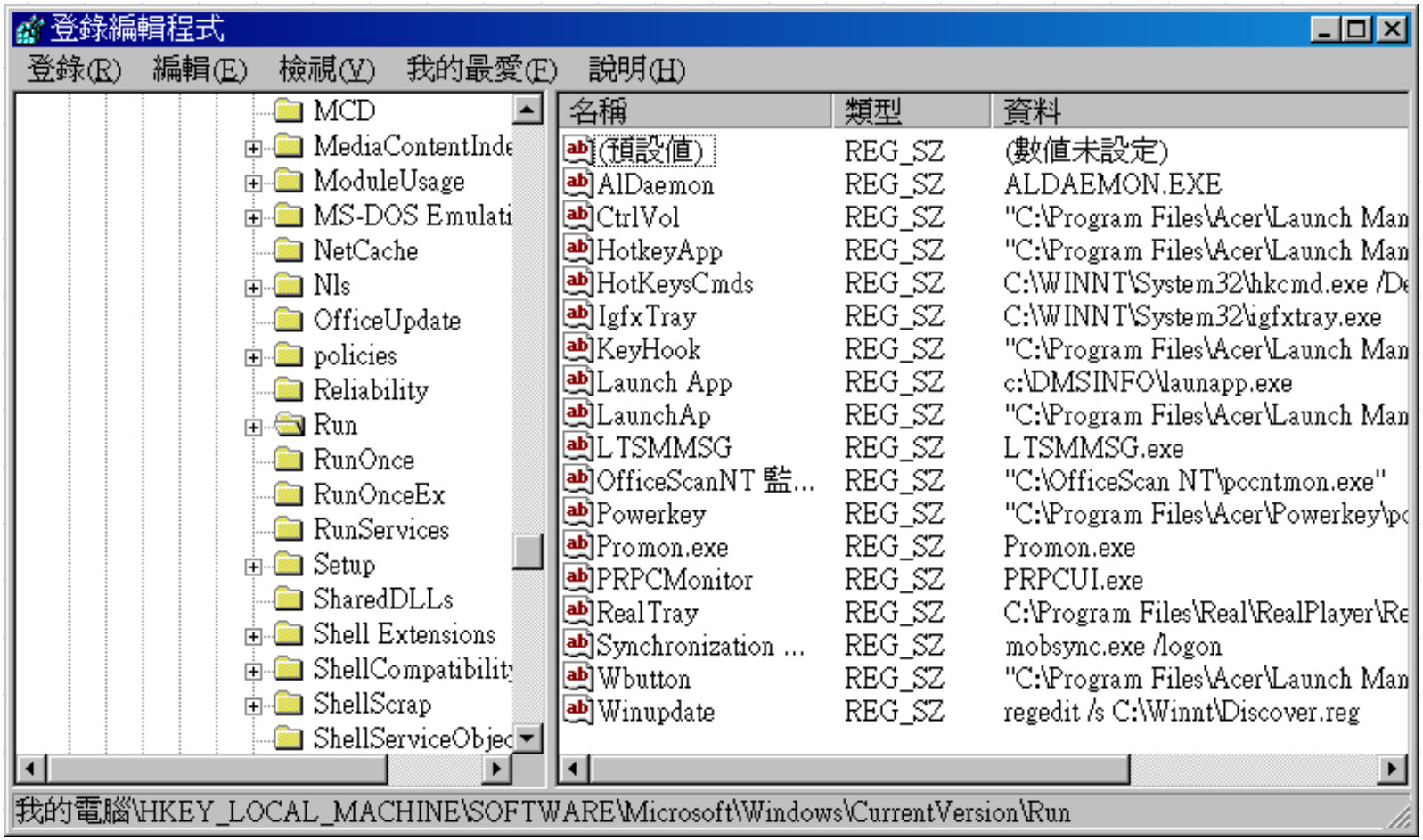


利用搜尋選項檢查檔案異動日期



登錄表（registry）

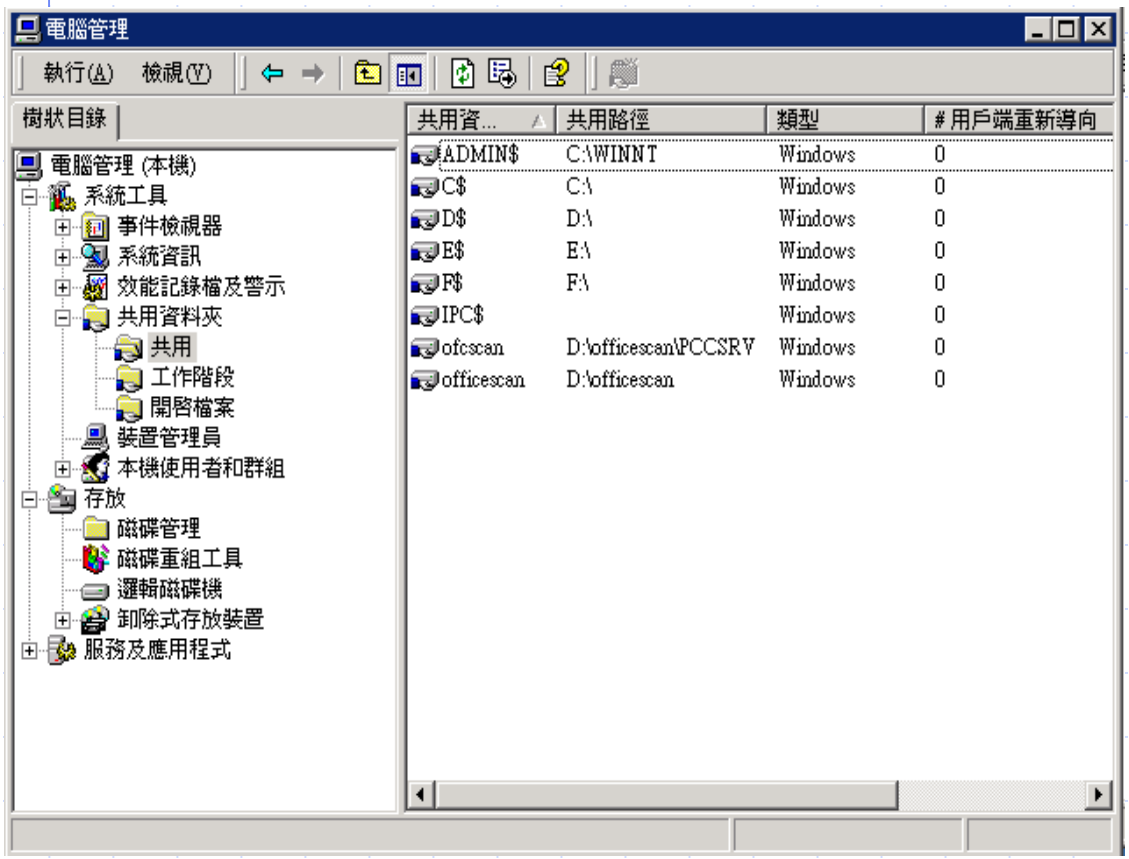
由 開始/執行 輸入regedit



登錄表檢查項目

- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion下之Run、RunOnce、RunServices是否不尋常的程式被啟動
- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows 之 AppInit_DLLs其資料欄應為空白
- \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogin之
  GinaDLL應該不存在
  Shell資料欄應為無路徑之Explorer.exe
  Userinit資料欄應為C:\WINNT\system32\userinit.exe (win2000) or C:\Windows\System32\userinit.exe (XP)

資源分享



開啟　開始／設定／控制台，點選 系統管理工具／電腦管理，於左邊之樹狀目錄，點選「共用資料夾」左邊之+符號，會展開「共用資料夾」下之子項目。

其中「共用」為share出去之目錄，請檢查是否有不必要之檔案分享。

「工作階段」為目前連上分享的來源。

「開啟檔案」為目前連上分享所開啟的檔案。

限制共享設定＊

- 關閉Windows2000/XP/2003系統預設並享
  \HKEY_LOCAL_MACHINE\CurrentControlSet\Services\Lanmanserver\parameters
  新增AutoShareWks:REG_DWORD:0
  (說明:以新增DWORD值,值的名稱為AutoShareWks,值為0)
  新增AutoShareServer:REG_DWORD:0

- 限制IPC$匿名存取的權限(預防匿名列舉帳號及密碼暴力破解)
  \HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Lsa
  新增RestrictAnonymous:REG_DWORD:1
  新增RestrictAnonymousSAM:REG_DWORD:1
  新增EveryoneIncludesAnonymous:REG_DWORD:0

事件檢視

開啟　開始／設定／控制台，點選 系統管理工具／事件檢視器，檢視是否有不正常事件

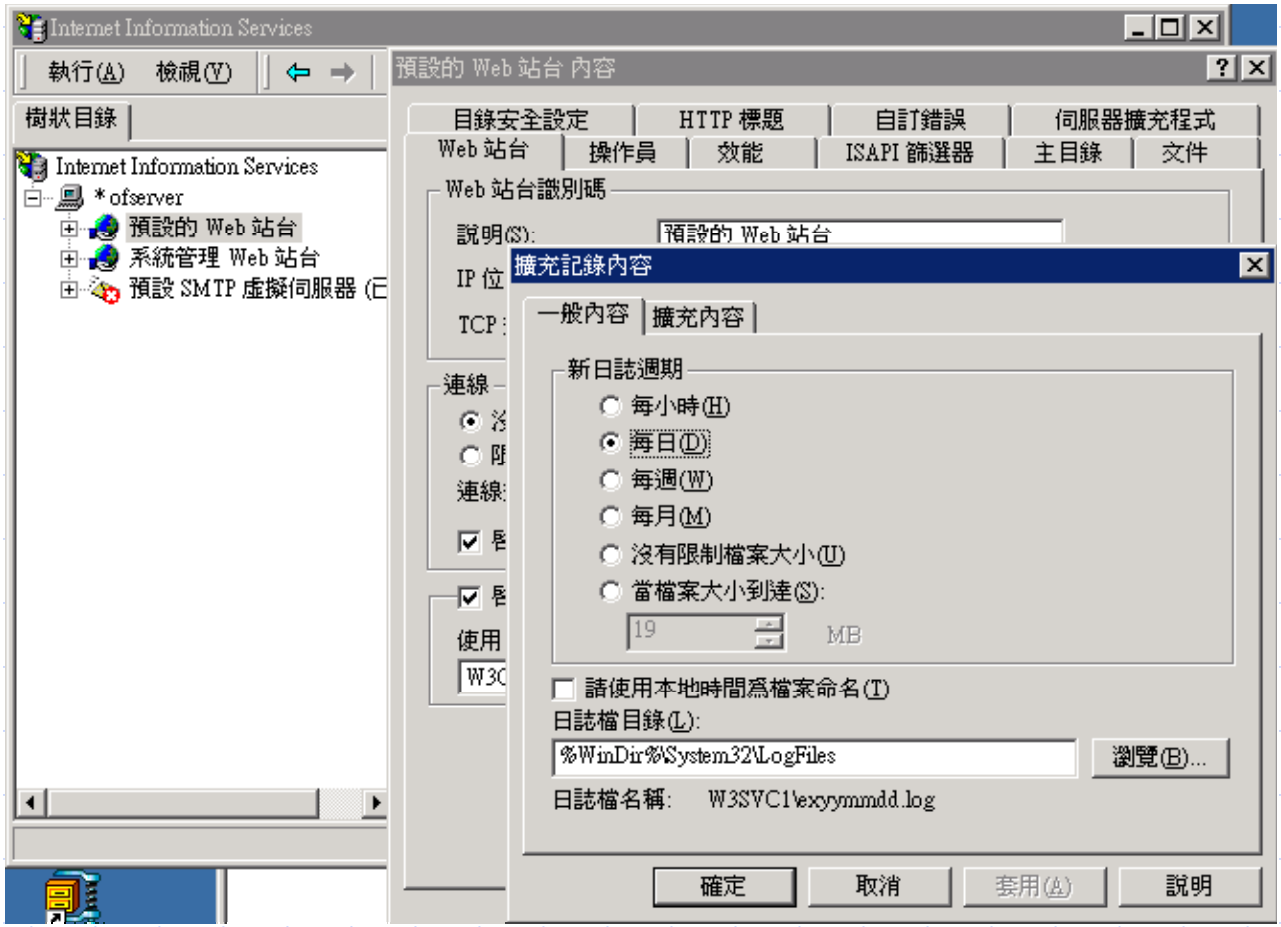
事件檢視之安全性記錄檔＊

開啟　開始／設定／控制台/系統管理工具/本機安全性原則，於其樹狀目錄欄之本機原則下之稽核原則，設定如下項目之設定值

即可在事件檢視之安全性記錄檔檢查如上項目之事件

Internet Services Logs＊

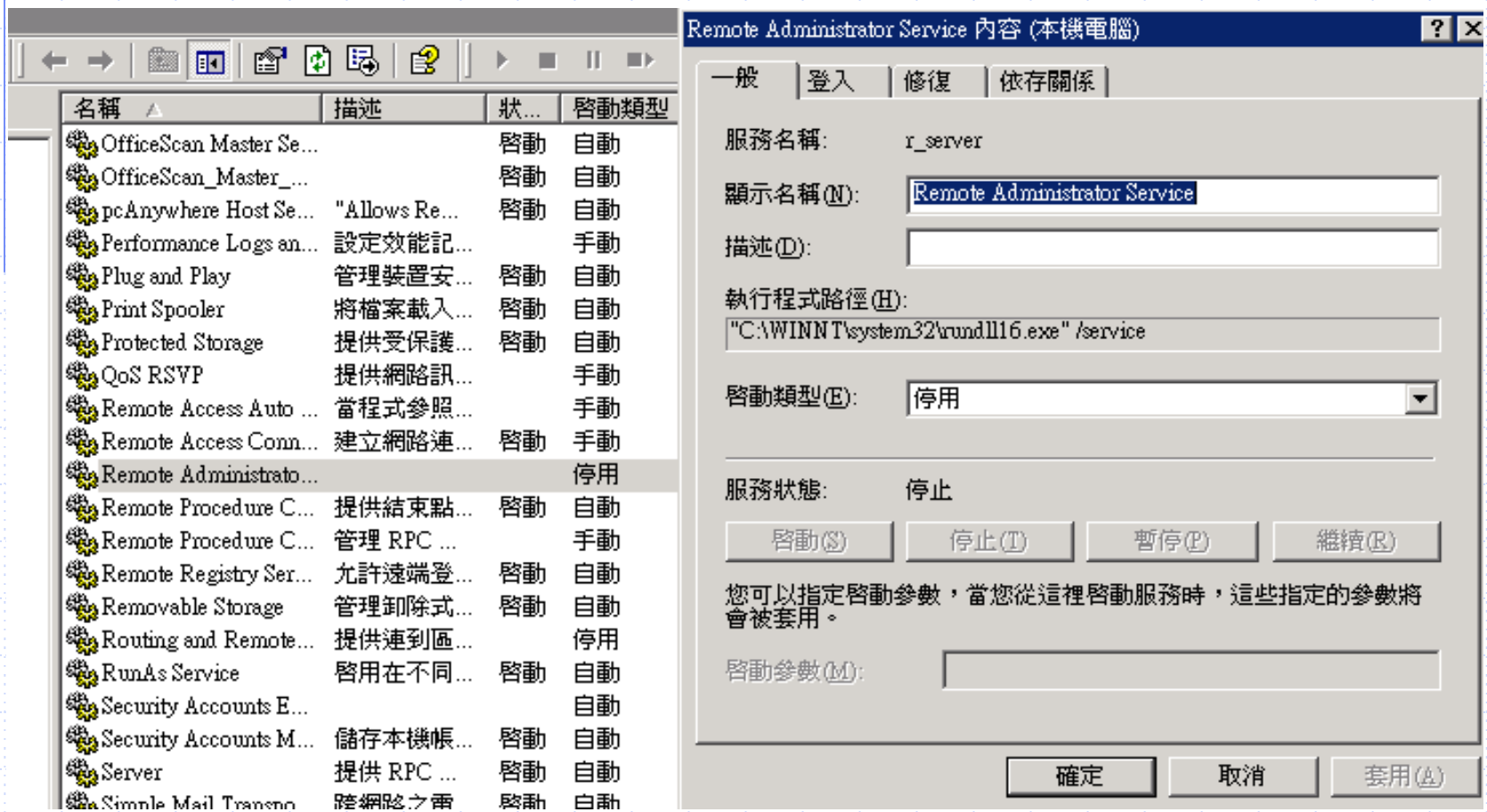
假如有開啟Internet（www、ftp 、smtp）Services，Log一般放置在/WINNT/system32/logFiles



Internet Services Logs

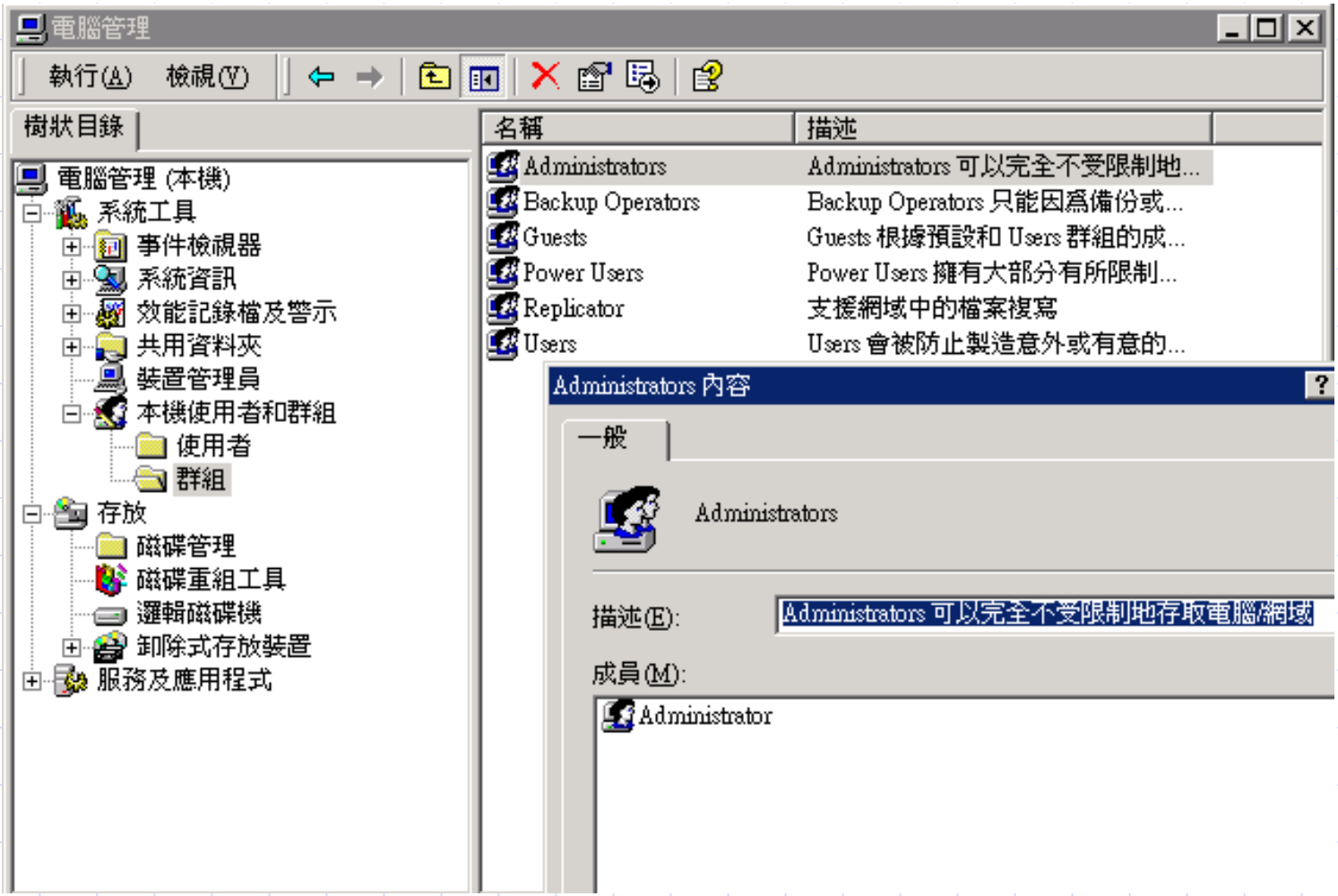
服務(Service)

至控制台／系統管理工具／服務 ,無描述，啟動類型為「自動」，狀態為「啟動」，顯示其內容之執行程式路徑，是否為遭植入的檔案



使用者帳號及其權限

是否有不明之使用者，一般使用者是否有administrator權限或群組



關於帳號

- Windows 登入必須設定密碼
- 移除guest帳號
- 注意不明帳號及Administrator群組之帳號
- 密碼設定不要過於簡單及英文單子，最好是大小寫數字及特殊符號混合設定

網頁綁架*

- 先取消IE之proxy，及點選 工具/網際網路選項/一般之Temporary Internet file之[刪除Cookie]及[刪除檔案]之按鍵
- 首頁被更改:
  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main及
  HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main 內名稱為“ Start Page ” 更改為首頁之網址
  進入
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 刪除值為“ internat.exe ”
  用regedit之搜尋原本被置放之網頁，並刪除
- 自動開啟到不知名的網站:
  以 Regedit找尋該網站的網址,若找到internat.exe 的機碼有該網址，刪除該網址,然後重新開機即可!!!

其他

- Autoexec.bat, Config.sys
- %windir%/win.ini 之 load= run =
- %windir%/system.ini 之 shall=
- 程式集／附屬應用程式／系統工具／排定的工作
- 程式集／啟動
- 硬碟是否被不正常使用