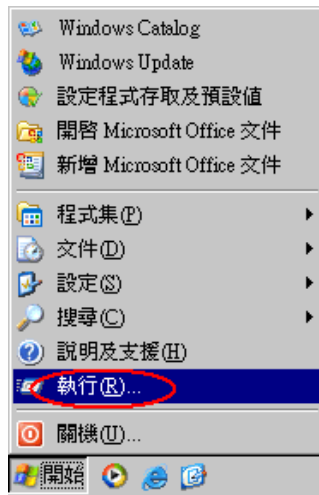


TCP 445 Port 中毒處理程序

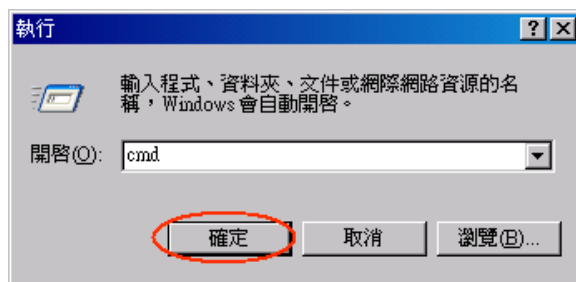
說明：移除網路芳鄰病毒，因病毒程式將檔案名稱隨機命名，故下列僅供參考。

操作步驟：

一、Windows 開始 → 執行

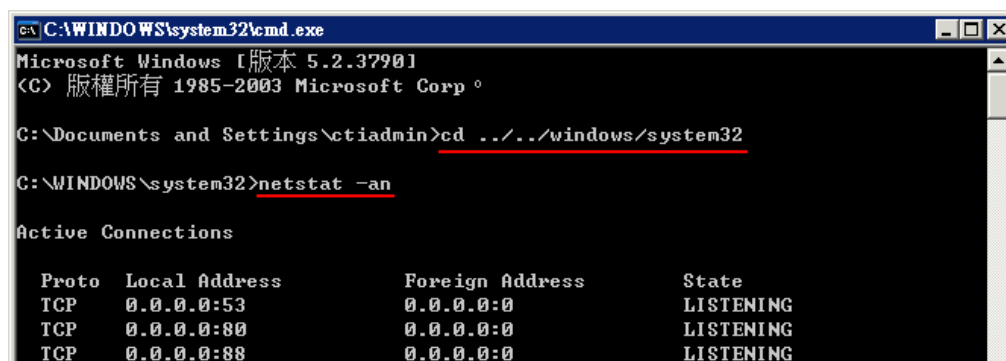


二、輸入 cmd → 點選 確定



三、檢查電腦目前對外連線狀況

1. 輸入 `cd ../../windows/system32`，切換到 system32 資料夾。
2. 輸入 `netstat -an`，查看本機是否有對外異常發送封包。

A screenshot of a Windows command prompt window. The title bar shows 'C:\WINDOWS\system32\cmd.exe'. The text in the window is as follows:

```
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\ctiadmin>cd ../../windows/system32
C:\WINDOWS\system32>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:53                0.0.0.0:0               LISTENING
TCP    0.0.0.0:80                0.0.0.0:0               LISTENING
TCP    0.0.0.0:88                0.0.0.0:0               LISTENING
```

3. 異常發送封包畫面如下，可看出本機持續發送封包到不明主機的 445 埠。

```

C:\WINDOWS\system32\cmd.exe
TCP 128.5.55.5:1324 128.5.55.5:389 ESTABLISHED
TCP 128.5.55.5:1346 128.5.55.4:1433 ESTABLISHED
TCP 128.5.55.5:1375 128.5.55.4:1433 ESTABLISHED
TCP 128.5.55.5:1384 12.113.134.12:445 SYN_SENT
TCP 128.5.55.5:1385 212.7.154.42:445 SYN_SENT
TCP 128.5.55.5:1386 135.48.193.19:445 SYN_SENT
TCP 128.5.55.5:1387 46.28.8.12:445 SYN_SENT
TCP 128.5.55.5:1388 179.79.112.51:445 SYN_SENT
TCP 128.5.55.5:1389 122.73.142.65:445 SYN_SENT
TCP 128.5.55.5:1390 102.68.173.22:445 SYN_SENT
TCP 128.5.55.5:1391 193.60.132.3:445 SYN_SENT
TCP 128.5.55.5:1392 220.78.194.31:445 SYN_SENT
TCP 128.5.55.5:1393 19.5.114.53:445 SYN_SENT
TCP 128.5.55.5:1394 68.107.66.12:445 SYN_SENT
TCP 128.5.55.5:1395 149.51.178.79:445 SYN_SENT
TCP 128.5.55.5:1396 177.5.64.116:445 SYN_SENT
TCP 128.5.55.5:1397 45.127.72.116:445 SYN_SENT
TCP 128.5.55.5:1398 151.35.87.108:445 SYN_SENT
TCP 128.5.55.5:1399 185.10.230.65:445 SYN_SENT
TCP 128.5.55.5:1400 214.122.25.55:445 SYN_SENT
TCP 128.5.55.5:1401 191.35.185.29:445 SYN_SENT
TCP 128.5.55.5:1402 82.16.106.19:445 SYN_SENT
TCP 128.5.55.5:1403 76.81.79.52:445 SYN_SENT
TCP 128.5.55.5:1404 152.23.111.98:445 SYN_SENT
TCP 128.5.55.5:1405 50.15.2.42:445 SYN_SENT
  
```

四、請在 ROOT 根目錄，輸入 `dir *.exe;*.dll;*.com /as /ah /s /tc`，查出異常的程式，例如：`utnpvub.dll`。

註 1：關於 `dir` 參數說明，可輸入 `dir /?` 查看。

註 2：因檔案名稱採隨機命名，可能查到的檔案不盡相同。

註 3：`NTDETECT.COM` 為正成常程式請勿移除。

```

C:\WINDOWS\system32>dir *.exe;*.dll;*.com /as /ah /s /tc
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: 7868-3E9F

C:\WINDOWS\system32 的目錄

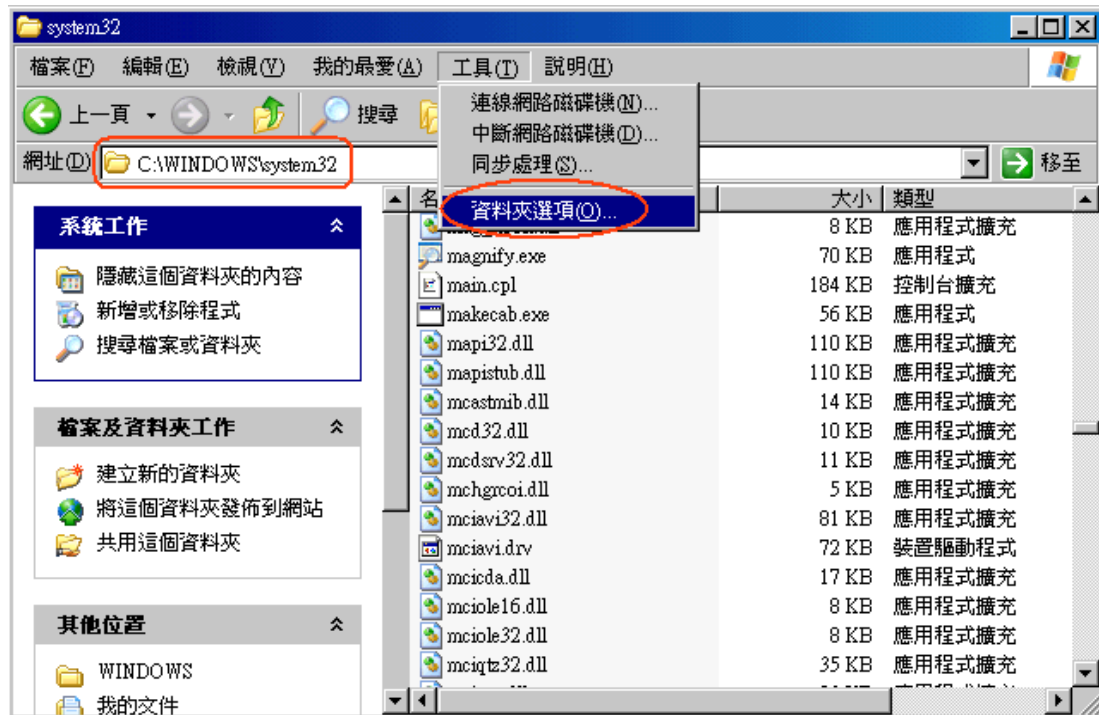
2007/04/19 上午 12:26          157,130 utnpvub.dll
                   1 個檔案          157,130 位元組

檔案數目總計:
                   1 個檔案          157,130 位元組
                   0 個目錄          59,574,173,696 位元組可用

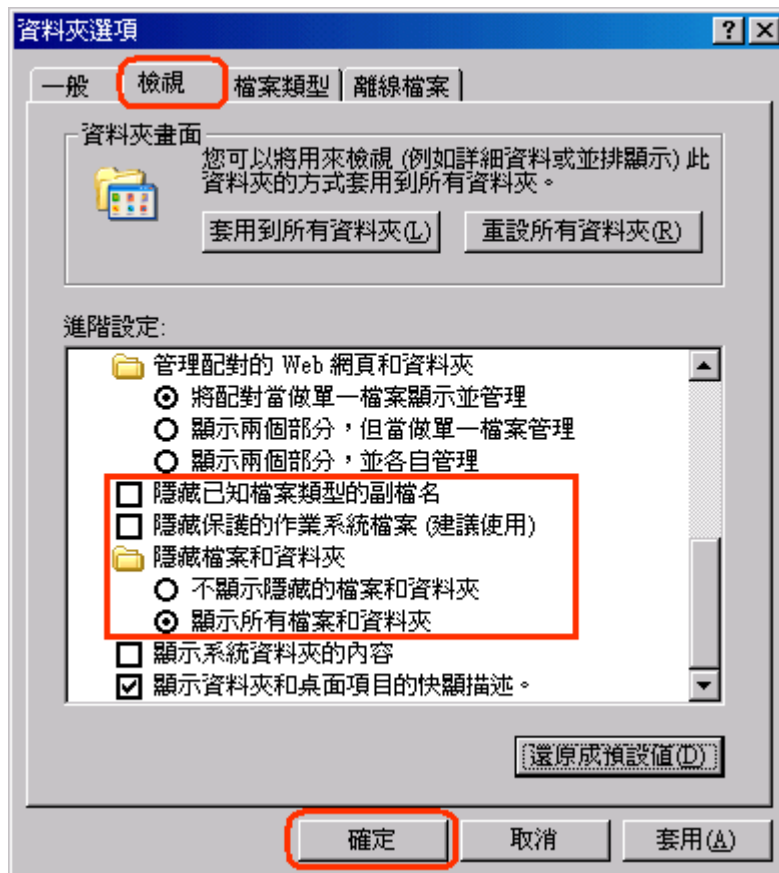
C:\WINDOWS\system32>
  
```

五、顯示系統隱藏檔

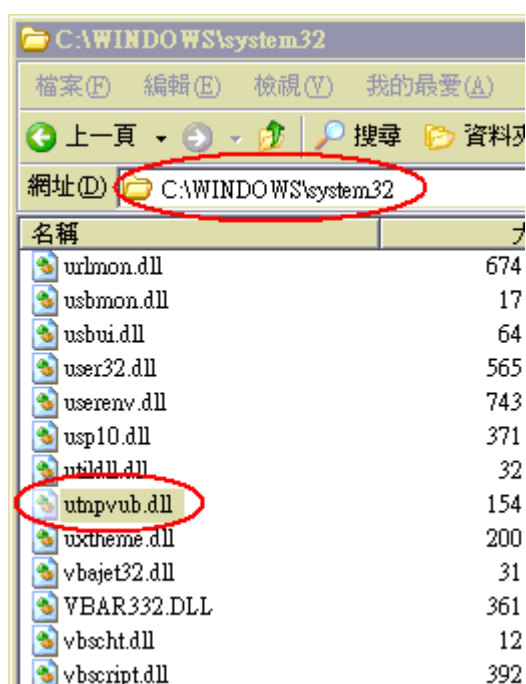
1. 將檔案總管切換到 `WINDOWS\system32` 的資料夾，選擇 `工具`，再點選 `資料夾選項`。



2. 切換到 檢視 頁籤，顯示所有檔案和資料夾，並點選 確定。



3. 找到 utnpvub.dll，因檔案被目前被系統鎖定，故無法刪除。

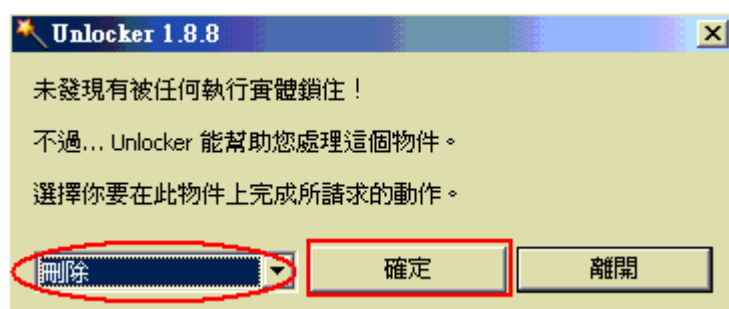


六、檔案解鎖

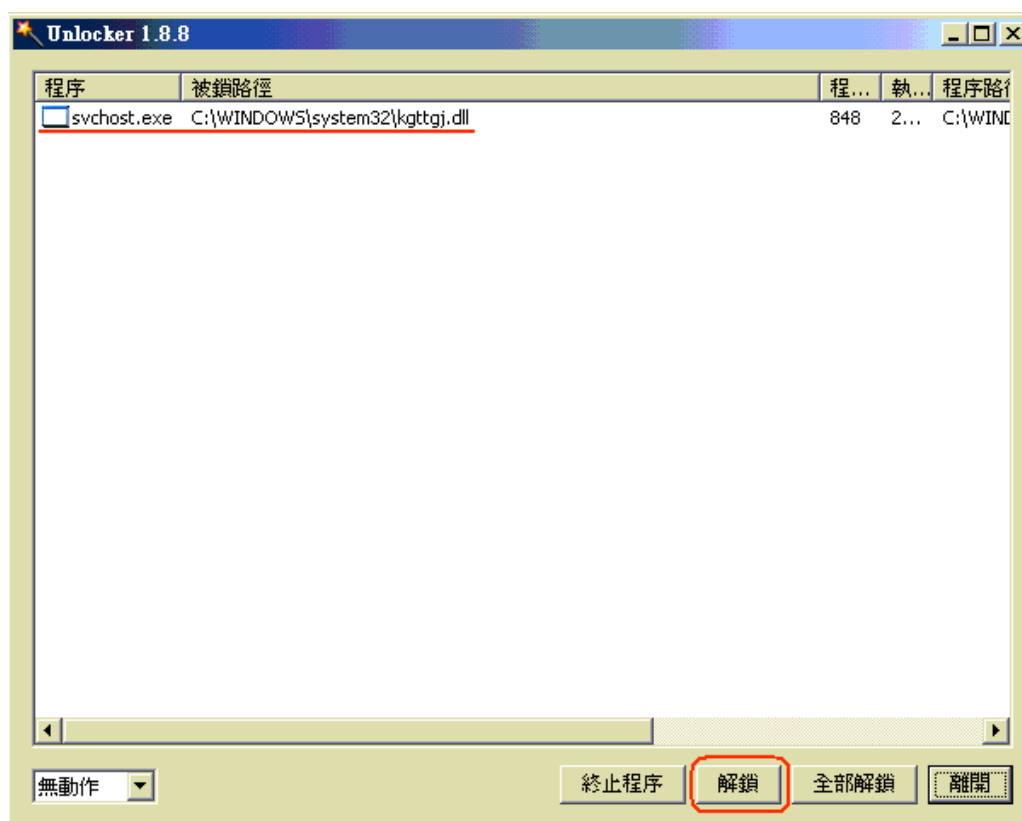
1. 下載 [Unlocker](http://www.softking.com.tw/) 程式，並安裝。(檔案來源：軟體王 <http://www.softking.com.tw/>)
2. 選擇要刪除的 dll 檔，點選滑鼠右鍵，選擇 **Unlocker**。



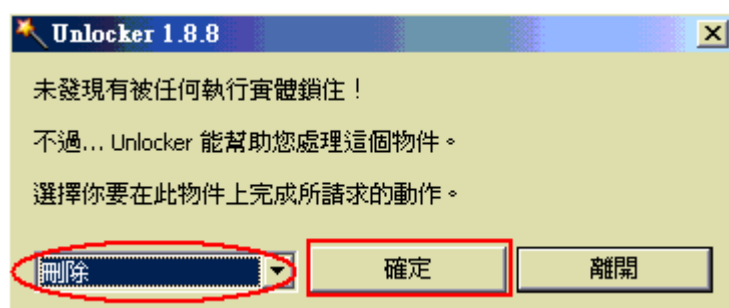
3. 若檔案未被任何程式鎖定，直接選擇 **刪除**，再點選 **確定**。



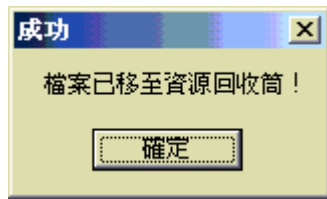
4. 若檔案被其他程式鎖定，則會列出程式名稱，請點選畫面下方 **解鎖**。



5. 再次點選 dll 檔，按滑鼠右鍵，選擇 **Unlocker**，物件已不被任何程式鎖定，直接選擇 **刪除**，再點選 **確定**。



6. 檔案成功刪除。



七、重新開機。

八、進入系統後，再次以 **netstat -an** 查看本機對外連線狀況，應已恢復正常。

九、更新防毒軟體，並確認已安裝 Windows 的所有安全性更新檔。