## 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

	Windows Catalog				
~	Williows Calaby				
-	Windows Update				
€	設定程式存取及預設値				
	開啓 Microsoft Office 文件				
<u>1</u>	新增 Microsoft Office 文件				
<b>6</b>	程式集(P)	►			
٨	文件(D)	⊁			
₽	設定(3)	⊁			
P	搜尋(C)	⊁			
0	說明及支援( <u>H</u> )				
	執行(R)				
0	關機(世)				
🦺開始 🕑 急 🕑					

二、輸入 cmd → 點選 確定

執行	? ×
-	輸入程式、資料夾、文件或網際網路資源的名 稱,Windows會自動開啓。
開啓(0):	cmd
	確定 取消 瀏覽 (B)

- 三、檢查電腦目前對外連線狀況
- 1. 輸入 cd ../../windows/system32,切换到 system32 資料夾。
- 2. 輸入 netstat -an,查看本機是否有對外異常發送封包。

C:\WINI	OOWS\system32\cmd.exe			_ 🗆 🗵			
Microsof <c>版權</c>	Microsoft Windows [版本 5.2.3790] <c>版權所有 1985-2003 Microsoft Corp。</c>						
C: Docum	ents and Settings\ctiad	min>cd//windows/sys	stem32				
C:\WINDO	WS\system32>netstat -an						
Active C	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				

C:\WI	NDOWS\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	-

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。

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。

🗁 system 32 📃 🖂 🗶							
檔案(F) 編輯(E) 檢視(V) 我的#	最愛(Δ) 工具(T) 說明(H)						
🚱 1 – j • 🕤 • 🏂 🔎	搜尋 🖟 連線網路磁碟機 (U) 中斷網路磁碟機 (D)						
網址① [ C:\WINDOWS\system32	同步處理(2)		💌 ラ 移至				
	▲ 名 溶料灰躍頂(0)	大小	類型   ▲				
系統工作	AHDORAO.	8 KB	應用程式擴充				
	💭 magnify.exe	70 KB	應用程式				
1 隐藏這個資料夾的內谷	🖃 main.cpl	184 KB	控制台擴充				
🛛 👸 新增或移除程式	📩 makecab.exe	56 KB	應用程式				
🔎 搜尋檔案或資料夾	🔊 mapi32.dll	110 KB	應用程式擴充				
	🔊 mapistub.dll	110 KB	應用程式擴充				
	🔊 mcəstmib.dll	14 KB	應用程式擴充				
檔案及資料夾工作 《	🔊 mcd.32.dll	10 KB	應用程式擴充 📃				
○→ 建立新的溶料本	🔊 mcdsrv32.dll	11 KB	應用程式擴充				
	🔊 mchgreoi.dll	5 KB	應用程式擴充				
🔇 將這個資料处發佈到網站	💳 💽 mciavi32.dll	81 KB	應用程式擴充				
😥 共用這個資料夾	📷 mciavi.drv	72 KB	裝置驅動程式				
	🕙 mcicda.dll	17 KB	應用程式擴充				
-++ AL 12 121	🔊 mciole16.dll	8 KB	應用程式擴充				
- 共把位直 *	🔊 mciole32.dll	8 KB	應用程式擴充				
🛅 WINDOWS	🔊 meiqtz 32.dll	35 KB	應用程式擴充				
🦳 我的文件	<b>▼</b> 4						

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 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 •
----	--------	--------	--------	-----	------------

名稱	大小	類型 🔺	修改日期	屬性
💁 urlmon.dll	674 KB	應用程式擴充	2007/8/18 下午 11:54	A
💁 usbmon.dll	17 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 usbui.dll	64 KB	應用程式擴充	2007/2/17 上午 06:52	A
🛐 user32.dll	565 KB	應用程式擴充	2007/3/2 下午 02:40	A
🛐 userenv.dll	743 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 usp10.dll	371 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 utild11.d11	32 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 utnpvub.dll	154 KB	應用程式擴充	2007/4/19 上午 12:26	RHSA
🕙 uxtheme.dll 🛛 関 督 畜 案 (且)	200 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 vbajet32.dn 🕰 Unlocker	31 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 VBAR332.1	361 KB	應用程式擴充	2000/4/26 下午 01:34	
Sovbscht.dll 傳送到(N)	• 12 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 vbscript.dll 👜 🗟 (T)	392 KB	應用程式擴充	2007/3/7 下午 08:00	A
vdmdbg.dll	25 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 vdmredir.dl 🛛 🕅 🕹 🕑	49 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 vds_ps.dll 建立捷徑(S)	30 KB	應用程式擴充	2007/3/7 下午 08:00	A
🕙 vdsbas.dll 🛛 刪除(D)	1 <i>3</i> 8 KB	應用程式擴充	2007/3/7 下午 08:00	A
🔊 vdsdyndr.dl 重新命名(M)	317 KB	應用程式擴充	2007/3/7 下午 08:00	A
S vdsutil.dll	61 KB	應用程式擴充	2007/3/7 下午 08:00	A
💊 ver.dll 内容(R)	9 KB	應用程式擴充	2007/3/7 下午 08:00	A

3. 若檔案未被任何程式鎖定,直接選擇 刪除,再點選 確定。

Unlocker 1.8.8			×				
未發現有被任何執行實體鎖(	注!						
不過 Unlocker 能幫助您處理	不過 Unlocker 能幫助您處理這個物件。						
選擇你要在此物件上完成所請求的動作。							
			<b>#488</b>				
	催疋		離開				

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。

*	Unlocker 1.8.	B		<u>- 🗆 ×</u>
	程序	被鎖路徑	程 執	程序路径
	svchost.exe	C:\WINDOWS\system32\kgttgj.dll	848 2	C:\WINE
	•			
	無動作 🗾		部解鎖	離開

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。