香港電腦保安事故協調中心
Hong Kong Computer Emergency Response Team Coordination

受 W32.Blaster 蠕蟲影響的視窗平台

- 視窗 NT 4.0, 視窗 2000 and 視窗 XP 操作系統

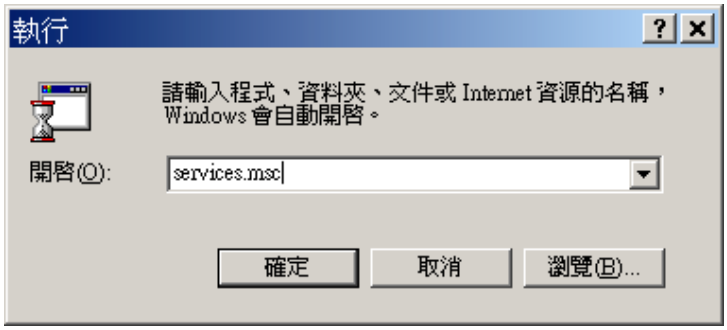
對付 W32.Blaster 蠕蟲的基本步驟 (第三版)

注意: 以下步驟**必須以擁有系統管員權限的帳戶執行，及必須全部順序執行**

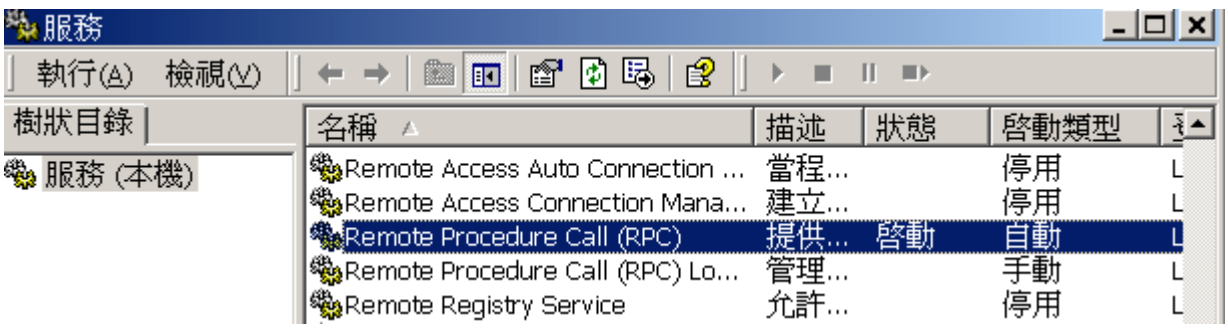
1. 停止 WinXP 機器不斷重新啓動 (Win2000 and WinNT 可略去此步驟)

視窗 XP 感染了 W32.Blaster 蠕蟲後，若連線就會不斷重新啓動。所以，要在離線時先改變視窗 XP 設定，停止機器不斷重新啓動，然後才安裝修補程式、掃描和清除蠕蟲等，最後，就是還原視窗 XP 設定。

- **先不要連接互聯網**。(如使用寬頻上網請關閉寬頻上網器的電源)
- 在 視窗 XP 工作列，按"開始" → 執行 → 開啓了執行視窗 → 在開啓中輸入 “services.msc” → 按 “確定”

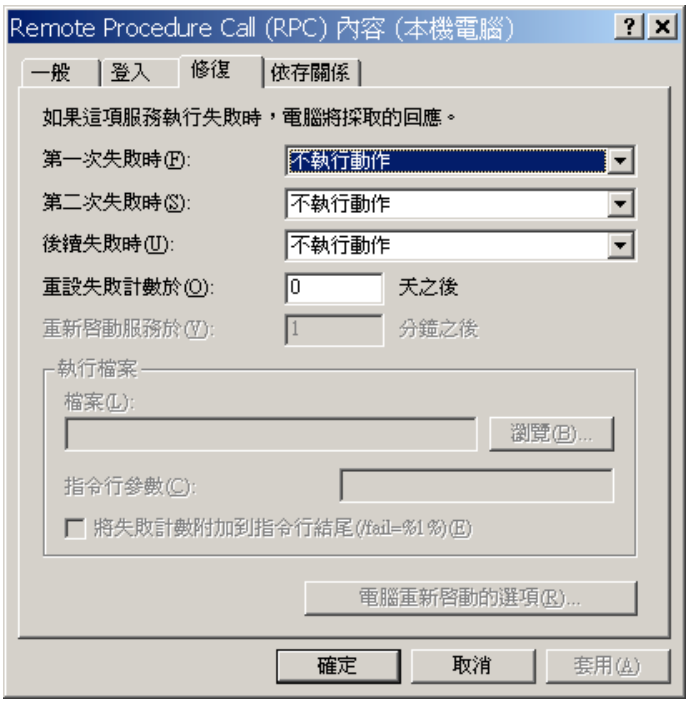


- 服務視窗出現，請找出 “Remote Procedure Call (RPC)” → 雙按"Remote Procedure Call (RPC)"



- “Remote Procedure Call (RPC) 內容” 視窗出現 → 選擇 “修復” → 將第一次失敗時, 第二

次失敗時和後續失敗時設爲 “**不執行動作**” → 按 “確定”



- 重新連接互聯網。(如使用寬頻上網請開啓寬頻上網器的電源)

2. 下載及安裝微軟 RPC 漏洞的修補程式

- 注意：
  最好在一部不受影響的系統 (視窗 98、視窗 ME) 或已修補好的系統下載修補程式，再經軟碟或光碟抄錄到受感染電腦上，這樣較爲安全。

- 緊記下面**祇選擇一個正確的視窗平台及語言去下載修補程式**

  視窗 NT 4.0 (英文):
  http://download.microsoft.com/download/6/5/1/651c3333-4892-431f-ae93-bf8718d29e1a/Q823980i.EXE

  視窗 NT 4.0 (繁體中文):
  http://download.microsoft.com/download/0/f/0/0f01962c-99a8-43d4-b0f9-5eca609a7ef1/CHTQ823980i.EXE

  視窗 NT 4.0 Terminal Server (英文):
  http://download.microsoft.com/download/4/6/c/46c9c414-19ea-4268-a430-53722188d489/Q823980i.EXE

  視窗 2000 (英文):
  http://download.microsoft.com/download/0/1/f/01fdd40f-efc5-433d-8ad2-b4b9d42049d5/Windows2000-KB823980-x86-ENU.exe

視窗 2000 (繁體中文):
http://download.microsoft.com/download/5/8/f/58fa7161-8db3-4af4-b576-0a56b0a9d8e6/Windows2000-KB823980-x86-CHT.exe

視窗 XP Home and 視窗 Professional 版本 (英文):
http://download.microsoft.com/download/9/8/b/98bcfad8-afbc-458f-aaee-b7a52a983f01/WindowsXP-KB823980-x86-ENU.exe

視窗 XP Home and 視窗 Professional 版本 (繁體中文):
http://download.microsoft.com/download/2/3/6/236eaaa3-380b-4507-9ac2-6cec324b3ce8/WindowsXP-KB823980-x86-CHT.exe

其他視窗平台：
http://www.microsoft.com/technet/security/bulletin/MS03-026.asp

- 下載完成後會開始安裝這修補程式，只選要按“下一步”直至“完成”。電腦會**重新啓動**。

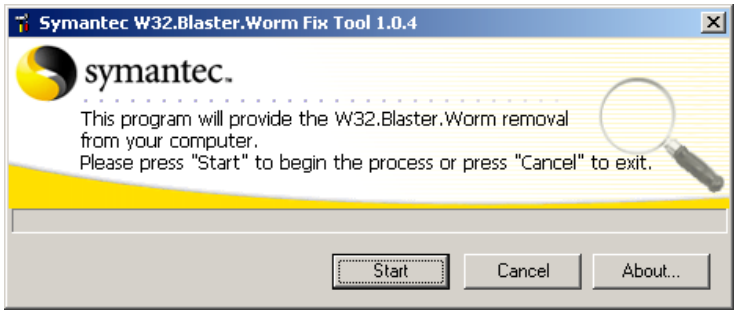
3. 掃描和清除蠕蟲

- 重新啓動之後，請預備一個 Symantec 的蠕蟲清除程式到桌面，留待稍後使用
  - 蠕蟲清除程式可到下面的網址下載：
    http://securityresponse.symantec.com/avcenter/FixBlast.exe
  - 注意:
    最好在一部不受影響的系統 (視窗 98、視窗 ME) 或已修補好的系統下載蠕蟲清除程式，再經軟碟或光碟抄錄到受感染電腦上，這樣較爲安全。
  - 下載時，選“儲存檔案” → 儲存至“桌面” → 按“儲存”

FixBlast.exe

- 視窗 XP 機器在執行蠕蟲清除程式前，先按下列步驟關閉"系統還原"： (視窗 2000 及視窗 NT 可略去此步驟)
  - 按“開始” → 對著“我的電腦”按滑鼠右鍵 → 選“內容”
  - “系統視窗”會出現 → 選“系統還原” → 選“**關閉系統還原**” → 選“確定” → 選“是”

- **重新啓動電腦** → 在開機時**不停地按“F8”**直至出現選舉列表 → 選“**安全模式**” → 進入“安全模式”後 → 執行桌面上“**FixBlast.exe**”

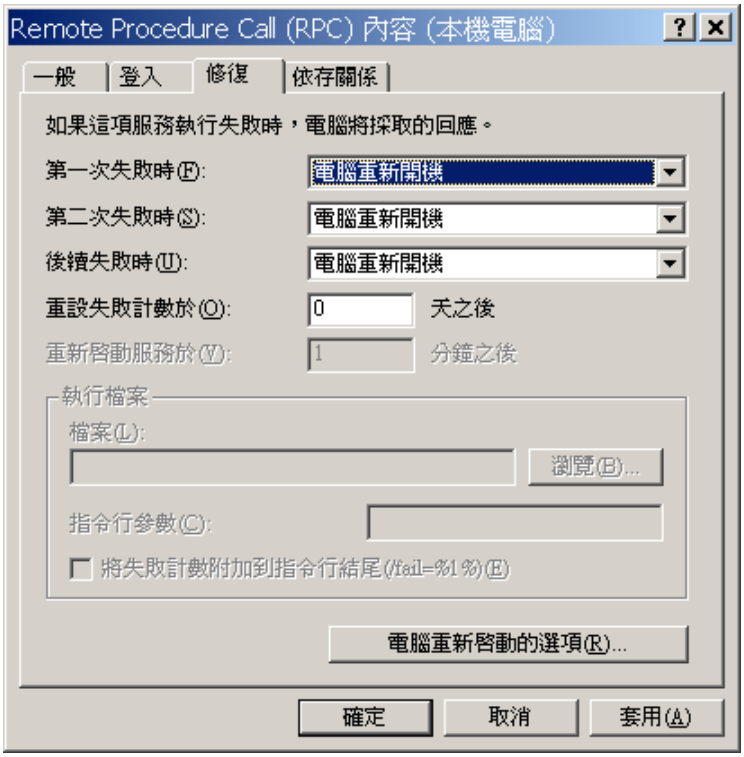


- 按 "**Start**" → 直至完成

- **重新啓動**電腦回**正常模式**

4. 還原 WinXP 設定 (Win2000 and WinNT 可略去此步驟)

- 按開始 → 執行 → 開啓了執行視窗 → 在開啓中輸入 "services.msc" → 按 "確定"
- 會出現服務視窗，請找出 "Remote Procedure Call (RPC)" → 雙按 "Remote Procedure Call (RPC)"
- 會出現"Remote Procedure Call (RPC) 內容" → 選擇 "修復" → 將第一次失敗時, 第二次失敗時和後續失敗時設爲 "**重新啓動電腦**" → 按 "確定"



- 按 "開始" → 對著 "我的電腦" 按滑鼠右鍵 → 選 "內容"
- 會出現 "系統視窗" → 選 "系統還原" → 選 "**關閉系統還原**" → 選 "確定" → 選 "是"
- 重新啓動電腦

至此，受感到染電腦應已修復。同時，因爲修補程式已堵塞 RPC 漏洞，就算有針對同一 RPC 漏洞的 W32.Blaster 新變種蠕蟲，機器也是防疫的了。

不過，下面的選擇性建議，可以進一步改善你的防禦工事。

對付 W32.Blaster 蠕蟲的選擇性建議步驟

5. 設定防火牆過濾網絡交通

- 若公司安裝有防火牆或帶有防火牆功能的寬頻路由器，可設定爲阻塞從互聯網進入存取 RPC 服務的交通，確保內部網絡上所有機器的安全，有效地減低公司的風險。需要在防火牆禁止的服務包括：
  - TCP/UDP 135
  - TCP/UDP 139
  - TCP/UDP 445

  此外，蠕蟲會使用到下面 2 個連接埠，都必須阻塞
  - UDP 69
  - TCP 4444

  如果不能禁止所有外來主機的存取，我們建議限制只允許日常操作所需的主機進行存取。根據良好的習慣，除日常操作需要的網絡交通以外，其他的網絡交通都應過濾。

- 家庭或個人電腦，也可使用帶有防火牆功能的寬頻路由器或個人防火牆軟件，達到以上目的。
  - **視窗 XP** 的電腦可啓動名叫 **"網際網路連線防火牆"** 的內建個人防火牆軟件，詳細步驟可參考以下網址：
    http://www.microsoft.com/taiwan/windowsxp/home/using/howto/homenet/icf.htm

--- 完 ---