

木馬的行爲介紹-Net bull

1. Peep 就是 Net bull 這支木馬程式，它跟一般木馬程式比較不一樣的地方是它是反過來運作，也就是裝在 User 端不是 Agent 而是 Sever，這樣一來它就在防火牆內部主動連線至外部的 Agent(外部駭客)，以避過防火牆的攔阻。
2. Net Bull 一共有下列幾支程式：peep.exe、peepviewer、buildsever、peepbrowser、peepsever、remove
3. 經測試後，發現它會主動用 80port 連線至外部的一個 IP 139。
4. 當主機被植入後，它會將原本的名字更換為 checkdll.exe，並且把這個檔案存放在 c:\winnt\system 中，它還會修改系統的 Registry，以便開機時會自動執行 checkdll.exe 這支程式。

如何清除 Net bull

1. 首先查看系統正在運行的 Process，如果有下列的項目，請先將它停止：
buildsever.exe peepsever.exe
peep.exe peepviewe.exe
remove.exe peppbrower
2. 搜尋系統中是否有上述的 6 個檔案，如果有的話請將它刪除，另外還有二個檔案 peepshell.dll、keycap.dll 如果有的話也一併刪除。
3. 查看系統的 Registry，如果有下列的值，請將它刪除：
[HKET_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
“CheckDll.exe”=”c:\WinDows\SYSTEM\CheckDll.exe”
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Services]
“CheckDll.exe”=”c:\WinDows\SYSTEM\CheckDll.exe”
[HEKY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]
“CheckDll.exe”=”c:\WinDows\SYSTEM\CheckDll.exe”
4. 如果系統中有 keycap.dll、peepshell.dll 這二支程式，還需要執行反註冊的程序：假設這二支程式在 c:\sinnt\system 中 Regsvr32-u c:\winnt\system\keycap.dll；
Regsvr32-u c:\winnt\system\peepshell.dll

木馬的行爲介紹－Twuuk_16

1. **Twuuk_16** 這支木馬目前在網路上查不到任何的資訊，也就是在一些安全軟體的木馬資料庫中並沒有它的特徵值，所以無法偵測到它的存在。
2. 經測後，它會主動用 **80 Port** 連線至以下的幾個 IP：
61.220.200.137
61.218.49.98
61.220.102.210
61.220.106.90
61.218.45.242
61.218.40.210
3. 當主機被植入後，它會將 **Twuuk_16.exe** 這支程式複製到 **c:\winnt\system** 中，並且檔案的屬性更改為隱藏、系統，因為系統本身的預設值就是不會顯示這二個屬性的檔案，所以一般使用者很難去發現到這個檔案的存在。

如何清除 Twuuk_16

1. 首先查看系統正在運行的 **Process**，如果有下列的項目，請先將它停止：
Twuuk_16.exe
2. 查看 **c:\winnt\system** 中是否有 **Twuuk_16.exe** 這支程式，如果有請將它刪除。
3. 查看系統中的 **Registry** 中，是否有下列值請將其刪除：
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
“twuuk_16.exe” =” c:\WinDOWS\SYSTEM\twuuk_16.exe”

木馬的行爲介紹－Services

1. **Services** 這支木馬跟系統中預設的程式 **services.exe** 名稱一模一樣，目前在網路上查不到任何的資訊，也就是在一些安全軟體的木馬資料庫中並沒有它的特徵值，所以無法偵測到它的存在。也因它的名稱是用系統中原本就有的檔案名稱，一般使用者很難去查覺。
2. 它會將本身的程式（**services.exe**）放在 `c:\winnt\system32\setup` 中，正常的 **services.exe** 是存放在 `c:\winnt\system32` 中。
3. 它會更改系統中的 **Registry**，讓開機時就會將它自動啓動。
4. 至於它的網路行爲尚在 **Lab** 中測試。

如何清除 Services

1. 查看 **Registry** 中是否有下列任一機碼，如果有的話請將它刪除：
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
“Services.exe”=”c:\Winnt\SYSTEM32\setup\Services.exe”
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
Services]
“Services.exe”=” c:\Winnt\SYSTEM32\setup\Services.exe”
2. 將機碼刪除重新開機後，將 **Services.exe** 這個檔案刪除。
註：一定要先刪機碼並重新開機後，才可刪除該檔案。

木馬的行爲介紹－Svchost

1. **Svchost** 這支木馬跟系統中預設的程式 **Svchost.exe** 名稱一模一樣，目前在網路上查不到任何的資訊，也就是在一些安全軟體的木馬資料中並沒有它的特徵值，所以無法偵測到它的存在。也因它的名稱是用系統中原本就有的檔案名稱，一般使用者很難去查覺。
2. 它會將本身程式（**Svchost.exe**）放在 **c:\winnt** 中，正常的 **Svchost** 是存放在 **c:\winnt\system32** 中。
3. 它會主動用 **80Port** 連線至下列的 IP：
61.220.57.10
61.221.104.67

如何清除 Svchost

1. 查看 **Registry** 中是否有下列任一機碼，如果有的話請將它刪除：
[HKET_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
“Svchost.exe”=”c:\Winnt\Svchost.exe”
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
“Svchost.exe”=”c:\Winnt\Svchost.exe”
[HEKY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]
“Svchost.exe”=”c:\Winnt\Svchost.exe”
2. 將機碼刪除重新開機後，將 **Services.exe** 這個檔案刪除。
註：一定要先刪機碼並重新開機後，才可刪除該檔案。