有很多新手對安全問題瞭解比較不多，電腦中了特洛伊木馬不知道怎麼樣來清除。雖然現在有很多的清除特洛伊木馬的軟體，可以自動清除木馬。但你不知道木馬是怎樣在電腦中運行的，如果你看了這篇文章之後，你就會明白一些木馬的原理。
雖然收集了很多木馬的資料，但我也不能保證全部正確。如果大家發現錯誤請及時於本站聯繫：網路安全 netsafe.ayinfo.ha.cn。
如果熱心的網友有木馬的資料，可以發對本站。謝謝大家的支援。
1. 冰河 v1.1　v2.2
這是國產最好的木馬　作者：黃鑫

清除木馬 v1.1
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
查找以下的兩個路徑，並刪除
" C:\windows\system\ kernel32.exe"
" C:\windows\system\ sysexplr.exe"
關閉 Regedit
重新啓動到 MSDOS 方式
刪除 C:\windows\system\ kernel32.exe 和 C:\windows\system\ sysexplr.exe 木馬程式
重新啓動。OK

清除木馬 v2.2
伺服器程式、路徑用戶是可以隨意定義，寫入註冊表的鍵名也可以自己定義。
因此，不能明確說明。
你可以察看註冊表，把可疑的文件路徑刪除。
重新啓動到 MSDOS 方式
刪除于註冊表相對應的木馬程式
重新啓動 Windows。OK

2. Acid Battery v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 Explorer ="C:\WINDOWS\expiorer.exe"
關閉 Regedit
重新啓動到 MSDOS 方式

刪除 c:\windows\expiorer.exe 木馬程式
注意：不要刪除正確的 ExpLorer.exe 程式，它們之間只有 i 與 L 的差別。
重新啓動。OK
3. Acid Shiver v1.0 + 1.0Mod + lmacid
清除木馬的步驟：

重新啓動到 MSDOS 方式
刪除 C:\windows\MSGSVR16.EXE
然後回到 Windows 系統
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 Explorer = "C:\WINDOWS\MSGSVR16.EXE"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
刪除右邊的 Explorer = "C:\WINDOWS\MSGSVR16.EXE"
關閉 Regedit
重新啓動。OK

重新啓動到 MSDOS 方式
刪除 C:\windows\wintour.exe 然後回到 Windows 系統
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 Wintour = "C:\WINDOWS\WINTOUR.EXE"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
刪除右邊的 Wintour = "C:\WINDOWS\WINTOUR.EXE"
關閉 Regedit
重新啓動。OK
4. Ambush
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的 zka = "zcn32.exe"
關閉 Regedit
重新啓動到 MSDOS 方式
刪除 C:\Windows\ zcn32.exe

重新啓動。OK
5. AOL Trojan
清除木馬的步驟：

啓動到 MSDOS 方式
刪除 C:\ command.exe（刪除前取消文件的隱含屬性）
注意：不要刪除真的 command.com 文件。
刪除 C:\ americ~1.0\buddyl~1.exe（刪除前取消文件的隱含屬性）
刪除 C:\ windows\system\norton~1\regist~1.exe（刪除前取消文件的隱含屬性）

打開 WIN.INI 文件
在[WINDOWS]下面"run="和"load="都載入者特洛伊木馬程式的路徑，必須清除它們：
run=
load=
保存 WIN.INI

還要改正註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 WinProfile = c:\command.exe
關閉 Regedit，重新啓動 Windows。OK
6. Asylum v0.1, 0.1.1, 0.1.2, 0.1.3 + Mini 1.0, 1.1
清除木馬的步驟：

注意：木馬程式默認檔案名是 wincmp32.exe，然而程式可以隨意改變檔案名。
我們可以根據木馬修改的 system.ini 和 win.ini 兩個文件來清除木馬。
打開 system.ini 文件
在[BOOT]下面有個"shell=檔案名"。正確的檔案名是 explorer.exe
如果不是"explorer.exe"，那麼那個文件就是木馬程式，把它查找出來，刪除。
保存退出 system.ini
打開 win.ini 文件
在[WINDOWS]下面有個 run=
如果你看到=後面有路徑檔案名，必須把它刪除。
正確的應該是 run=後面什麼也沒有。
=後面的路徑檔案名就是木馬，把它查找出來，刪除。
保存退出 win.ini。
OK
7. AttackFTP

清除木馬的步驟：

打開 win.ini 文件
在[WINDOWS]下面有 load=wscan.exe
刪除 wscan.exe ，正確是 load=
保存退出 win.ini。

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 Reminder="wscan.exe /s"
關閉 Regedit，重新啓動到 MSDOS 系統中
刪除 C:\windows\system\ wscan.exe
OK
8. Back Construction 1.0 - 2.5
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的"C:\WINDOWS\Cmctl32.exe"
關閉 Regedit，重新啓動到 MSDOS 系統中
刪除 C:\WINDOWS\Cmctl32.exe
OK
9. BackDoor v2.00 - v2.03
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的'c:\windows\notpa.exe /o=yes'
關閉 Regedit，重新啓動到 MSDOS 系統中
刪除 c:\windows\notpa.exe
注意：不要刪除真正的 notepad.exe 筆記本程式
ＯＫ
10. BF Evolution v5.3.12
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的(Default)=" "
關閉 Regedit，再次重新啓動電腦。
將 C:\windows\system\ .exe（空格 exe 文件）
ＯＫ
11. BioNet v0.84 - 0.92 + 2.21

0.8X 版本是運行在 Win95/98
0.9X 以上版本有運行在 Win95/98 和 WinNT 上兩個軟體
客戶－伺服器協定是一樣的，因而 NT 客戶能黑 95/98 被感染的機器，和 Win95/98 客戶能黑 NT 被感染的系統完全一樣。
清除木馬的步驟：
首先準備一張 98 的啓動盤，用它啓動後，進入 c:\windows 目錄下，用 attrib libupd~1.exe -h
命令讓木馬程式可見，然後刪除它。
抽出軟碟後重新啓動，進入 98 下，在註冊表裏找到：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
的子鍵 WinLibUpdate = "c:\windows\libupdate.exe -hide"
將此子鍵刪除。

12. Bla v1.0 - 5.03
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 Systemdoor = "C:\WINDOWS\System\mprdll.exe"
關閉 Regedit，重新啓動電腦。
查找到 C:\WINDOWS\System\mprdll.exe 和
C:\WINDOWS\system\rundll.exe
注意：不要刪除 C:\WINDOWS\RUNDLL.EXE 正確文件。
並刪除兩個文件。
OK
13. BladeRunner
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
可以找到 System-Tray = "c:\something\something.exe"
右邊的路徑可能是任何東西，這時你不需要刪除它，因爲木馬會立即自動加上，你需要的是記下木馬的名字與目錄，然後退回到 MS-DOS 下，找到此木馬文件並刪除掉。
重新啓動電腦，然後重復第一步，在註冊表中找到木馬文件並刪除此鍵。
14. Bobo v1.0 - 2.0
清除木馬 v1.0
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
刪除右邊的 DirrectLibrarySupport ="C:\WINDOWS\SYSTEM\Dllclient.exe"
關閉 Regedit，重新啓動電腦。
DEL C:\Windows\System\Dllclient.exe
OK

清除木馬 v2.0
打開註冊表 Regedit
點擊目錄至：
HKEY_USER/.Default/Software/Mirabilis/ICQ/Agent/Apps/ICQ Accel/
ICQ Accel 是一個“假像“的主鍵，選中 ICQ Accel 主鍵並把它刪除。
重新啓動電腦。OK
15. BrainSpy vBeta
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
右邊有 ??? = "C:\WINDOWS\system\BRAINSPY .exe"
???標簽選是隨意改變的。
關閉 Regedit，重新啓動電腦
查找刪除 C:\WINDOWS\system\BRAINSPY .exe
ＯＫ
16. Cain and Abel v1.50 - 1.51
這是一個口令木馬

進入 MS-DOS 方式
查找到 C:\windows\msabel32.exe
並刪除它。ＯＫ
17. Canasson
清除木馬的步驟：

打開 WIN.INI 文件
查找 c:\msie5.exe，刪除全部主鍵
保存 win.ini
重新啓動電腦
刪除 c:\msie5.exe 木馬文件
ＯＫ
18. Chupachbra
清除木馬的步驟：

打開 WIN.INI 文件
[Windows]的下面有兩個行
run=winprot.exe
load=winprot.exe
刪除 winprot.exe
run=
load=
保存 Win.ini，再打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
刪除右邊的'System Protect' = winprot.exe
重新啓動 Windows
查找到 C:\windows\system\ winprot.exe，並刪除。
ＯＫ
19. Coma v1.09
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
刪除右邊的'RunTime' = C:\windows\msgsrv36.exe
重新啓動 Windows
查找到 C:\windows\ msgsrv36.exe，並刪除。

ＯＫ
20. Control
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
刪除右邊的 Load MSchv Drv = C:\windows\system\MSchv.exe
保存 Regedit，重新啓動 Windows
查找到 C:\windows\system\MSchv.exe，並刪除。
ＯＫ
21. Dark Shadow
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\RunServices
刪除右邊的 winfunctions="winfunctions.exe"
保存 Regedit，重新啓動 Windows
查找到 C:\windows\system\ winfunctions.exe，並刪除。
ＯＫ
22. DeepThroat v1.0 - 3.1 + Mod (Foreplay)
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
版本 1.0
刪除右邊的專案'System32'=c:\windows\system32.exe
版本 2.0-3.1
刪除右邊的專案'SystemTray' = 'Systray.exe'
保存 Regedit，重新啓動 Windows
版本 1.0 刪除 c:\windows\system32.exe
版本 2.0-3.1
刪除 c:\windows\system\systray.exe
ＯＫ
23. Delta Source v0.5 - 0.7
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
刪除右邊的專案：DS admin tool = C:\TEMPSERVER.exe
保存 Regedit，重新啓動 Windows
查找到 C:\TEMPSERVER.exe，並刪除它。
ＯＫ
24. Der Spaeher v3
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
刪除右邊的專案：explore = "c:\windows\system\dkbdll.exe "
保存 Regedit，重新啓動 Windows
刪除 c:\windows\system\dkbdll.exe 木馬文件。
ＯＫ
25. Doly v1.1 - v1.7 (SE)
清除木馬 V1.1-V1.5 版本：

這幾個木馬版本的木馬程式放在三處，增加二個註冊專案，還增加到 Win.ini 專案。
首先，進入 MS-DOS 方式，刪除三個木馬程式，但 V1.35 版本多一個木馬文件 mdm.exe。
把下列各項全部刪除：
C:\WINDOWS\SYSTEM\tesk.sys
C:\WINDOWS\Start Menu\Programs\Startup\mstesk.exe
c:\Program Files\MStesk.exe
c:\Program Files\Mdm.exe
重新啓動 Windows。

接著，打開 win.ini 文件
找到[WINDOWS]下面 load=c:\windows\system\tesk.exe 專案，刪除路徑，改變爲 load=
保存 win.ini 文件。

最後，修改註冊表 Regedit
找到以下兩個專案並刪除它們
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Ms tesk = "C:\Program Files\MStesk.exe"

和
HKEY_USER\.Default\Software\Microsoft\Windows\CurrentVersion\Run
Ms tesk = "C:\Program Files\MStesk.exe"
再尋找到 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ss
這個組是木馬的全部參數選擇和設置的伺服器，刪除這個 ss 組的全部專案。
關閉保存 Regedit。
還有打開 C:\AUTOEXEC.BAT 文件，刪除
@echo off copy c:\sys.lon c:\windows\StartMenu\Startup Items\
del c:\win.reg
關閉保存 autoexec.bat。
ＯＫ

清除木馬 V1.6 版本：
該木馬運行時，將不能通過 98 的正常操作關閉，只能 RESET 鍵。徹底清除步驟如下：
1．打開控制面板——添加刪除程式——刪除 memory manager 3.0，這就是木馬程式，但是它並不會把木馬的 EXE 文件刪除掉。
2．用 98 或 DOS 啓動盤啓動（用 RESET 鍵）後，轉入 C:\，編輯 AUTOEXEC。BAT，把如下內容刪除：
@echo off copy c:\sys.lon c:\windows\startm~1\programs\startup\mdm.exe
del c:\win.reg
保存 AUTOEXEC。BAT 文件並返回 DOS 後，在 C：\根目錄下刪除木馬文件：
del sys.lon
del windows\startm~1\programs\startup\mdm.exe
del progra~1\mdm.exe
3．抽出軟碟重新啓動，進入 98 後，把 c:\program files\目錄下的 memory manager 目錄刪除。

清除木馬 V1.7 版本：
首先，打開 C:\AUTOEXEC.BAT 文件，刪除
@echo off copy c:\sys.lon c:\windows\startm~1\programs\startup\mdm.exe
del c:\win.reg
關閉保存 autoexec.bat

然後打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\MicroSoft\Windows\CurrentVersion\Run
找到 c:\windows\system\mdm.exe 路徑並刪除這個專案
點擊目錄至：

HKEY_USER/.Default/Software/Marabilis/ICQ/Agent/Apps/
找到"C:\windows\system\kernal32.exe"路徑並刪除這個專案
關閉保存 Regedit。重新啓動 Windows。

最後，刪除以下木馬程式：
c:\sys.lon
c:\iecookie.exe
c:\windows\start menu\programs\startup\mdm.exe
c:\program files\mdm.exe
c:\windows\system\mdm.exe
c:\windows\system\kernal32.exe
注意：kernal32 是Ａ
ＯＫ

26. Donald Dick v1.52 - 1.55
清除木馬 V1.52-1.53 版本：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\VxD\VMLDIR\
刪除右邊的專案：StaticVxD = "vmldir.vxd"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\System\vmldir.vxd
ＯＫ

清除木馬 V1.54-1.55 版本：

這兩個版本跟上面的版本只是默認檔案名不同，其他都一樣，
把 vmldir.vxd 改爲 intld.vdx 即可。
27. Drat v1.0 - 3.0b
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：hkey_classes_root\exefile\shell\open\command
找到@=SHELL32 \"%1\" %*把它更改爲@="%1" %*
關閉保存 Regedit，重新啓動 Windows。
查找 c:\windows\下 shell32・＊文件，並刪除它。
ＯＫ

28. Eclipse 2000
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：bybt = "c:\windows\system\eclipse2000.exe"
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ RunServices\
刪除右邊的專案：cksys = "c:\windows\system\ could be anything .exe"
關閉保存 Regedit，重新啓動 Windows
查找到 eclipse2000.exe 木馬文件，並刪除。
ＯＫ
29. Eclypse v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Rnaapp ="C:\WINDOWS\SYSTEM\rmaapp.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\SYSTEM\rmaapp.exe
注意：不要刪除 Rnaapp.exe
ＯＫ
30. Executer v1
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
在右邊的專案查找到"C:\windows\sexec.exe"，並刪除。
關閉保存 Regedit，重新啓動 Windows
相應刪除木馬程式文件。
ＯＫ
31. FakeFTP beta
清除木馬的步驟：

打開註冊表 Regedit

點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Rundll32 = rundll3.tww /h
關閉保存 Regedit，重新啓動 Windows
找到 C:\windows\文件夾下的三個文件並刪除它們
rundll3.bat - 9x.reg - nt.reg
ＯＫ
32. Forced Entry
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：MicrosoftRegistration32 = "C:\somepath \trojanhrs.exe"
關閉保存 Regedit，重新啓動 Windows
由於路徑容易改變，只要查找到 trojanhrs.exe，並刪除它。
33. GateCrasher v1.0 - 1.2
清除木馬 v1.0：
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Explore='c:\windows\explore.exe'
關閉保存 Regedit，重新啓動 Windows
然後，刪除相應的木馬程式。
ＯＫ

清除木馬 v1.1：
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Inet='EXPLORE.EXE'
關閉保存 Regedit，重新啓動 Windows
然後，找到相應的木馬程式，並刪除。
ＯＫ

清除木馬 v1.2：
打開註冊表 Regedit
點擊目錄至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Command = 'c:\windows\system.exe'

關閉保存 Regedit，重新啓動 Windows
然後，找到相應的木馬程式，並刪除。
ＯＫ
34. Girlfriend v1.3x (Including Patch 1 and 2)
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Windll.exe ="C:\windows\windll.exe"
Regedit 裏也保存著伺服器的資料
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\General
刪除 General 專案標題
關閉保存 Regedit，重新啓動 Windows
然後，找到相應的木馬程式，並刪除。
ＯＫ
35. Golden Retreiver v1.1b
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Task Manager="c:\mstask.exe"
關閉保存 Regedit，重新啓動 Windows
然後，找到相應的木馬程式，並刪除。
ＯＫ
36. Hack`a`Tack 1.0 - 2000
清除木馬 v1.0-1.2：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Explorer32 ="C:\windows\Expl32.exe"
關閉保存 Regedit，重新啓動 Windows
然後，找到相應的木馬程式，並刪除。

ＯＫ

清除木馬 v2000：
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Configuration Wizard = c:\windows\cfgwiz32.exe
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\cfgwiz32.exe
ＯＫ
37. Hack99 KeyLogger
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：HKeyLog = "C:\Windows\System\HKeyLog.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\Windows\System\HKeyLog.exe
ＯＫ
38. HostControl v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：RegClean = "c:\windows\inf\regcle32.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\inf\regcle32.exe
ＯＫ
39. Hvl Rat v5.30
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Explorer = "C:\WINDOWS\system\MSGSVR16.EXE"
關閉保存 Regedit，重新啓動 Windows

刪除 C:\WINDOWS\system\MSGSVR16.EXE
ＯＫ
40. ik97 v1.2
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：ik = 'c:\progra~1\ik\ik.exe'
關閉保存 Regedit，重新啓動 Windows
刪除 C:\Program Files\ik\ik.exe
ＯＫ
41. InCommand v1.0 - 1.5
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
找到右邊的專案：AdvancedSettings = *
注意：*表示就是木馬的存放路徑與檔案名，記下後刪除此鍵。
關閉保存 Regedit，重新啓動 Windows
按照剛才記下的木馬路徑與檔案名刪除木馬程式。
42. IndocTrination v0.1 - v0.11
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
Once\
每項標題都包括 Msgsrv16 ="Msgsrv16"專案
刪除每個專案
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\msgserv16.exe
ＯＫ
43. inet v2.0 - 2.0n

清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Explorer = "C:\WINDOWS\system\inet.exe"
關閉保存 Regedit，重新啓動 Windows
刪除"C:\WINDOWS\system\inet.exe"
刪除"C:\WINDOWS\system\inet.dll"
ＯＫ
44. Infector v1.0 - 1.42
清除木馬的步驟：

打開 system.ini 文件
找到 shell=explorer.exe c:\path\to\trojan.exe 專案
改爲：shell=explorer.exe
保存關閉 system.ini 文件，重新啓動 Windows
刪除 c:\path\to\trojan.exe
ＯＫ
45. iniKiller v1.2 - 3.2 Pro
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Explore="C:\windows\bad.exe "
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\bad.exe
ＯＫ
46. Intruder
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：PPModule1 = 'ppmod1.sys'
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\ ppmod1.sys

刪除 C:\windows\system\ ppmod2.sys
ＯＫ
47. IRC3
清除木馬的步驟：

打開 win.ini 文件
找到 load=closew 專案，更改爲：load=
保存關閉 win.ini，重新啓動 Windows
查找這兩個文件'rundlls.exe' 、'closew.bat'
並刪除它們。
ＯＫ
48. Kaos v1.1 - 1.3
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Sys="c:\windows\shell32.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\shell32.exe
ＯＫ
49. Khe Sanh v2.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：TBoot0001="c:\windows\system\trjp.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\system\trjp.exe
ＯＫ
50. Kuang logger
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：K2logas.task ="C:\WINDOWS\SYSTEM\K2logas.exe"

關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\SYSTEM\K2logas.exe
ＯＫ
51. Kuang Original - 0.34
清除木馬 v Original 版本：
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Temp$1.task = "c:\windows\system\temp$1.exe"
清除木馬 v 0.20-0.21 版本：
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：K2PS.task = "c:\windows\system\k2ps.exe"
清除木馬 v 0.30-0.34 版本：
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：K2PS_full.task = "c:\windows\system\k2ps_full.exe"

關閉保存 Regedit，重新啓動 Windows
查找相對應的木馬程式，並刪除。
ＯＫ
52. Logger
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：??? = "C:\windows\system\logged.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\SYSTEM\ logged.exe
ＯＫ
53. Magic Horse
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SpoolerService="c:\windows\spoolsrv.exe"

關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\spoolsrv.exe
ＯＫ
54. Malicious
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Policies\
刪除右邊的五個專案：DisableRegistryTools NoRun NoFind NoDesktop NoClose
關閉保存 Regedit，重新啓動 Windows
OK
55. Masters Paradise
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SYSEDIT = c:\windows\ sysedit.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
刪除右邊的專案：Explorer = c:\.....\agent.exe
關閉保存 Regedit，重新啓動 Windows
查找到木馬程式，並刪除它們。
注意：c:\windows\system\下面的 sysedit.exe 文件是不是 19KB，如果不是說明以被木馬感染，刪除它。
ＯＫ
56. Matrix v1.0 - 2.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：??? ="C:\WINDOWS\Wincfg.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\Wincfg.exe
ＯＫ
57. MBK
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
查找並刪除右邊的專案：Explorer =" "後面是"mbt.exe"
關閉保存 Regedit，重新啓動 Windows
查找 mbt.exe 並刪除
ＯＫ
58. Millenium v1.0 - 2.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Millenium = "C:\windows\system\reg66.exe "
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\reg66.exe
ＯＫ
59. Mine
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案： Windows = 'c:\msdos98.exe'
關閉保存 Regedit，重新啓動 Windows
刪除 c:\msdos98.exe
打開 win.ini 文件
查找到 run=c:\windows\uninstallms.exe
更改爲：run=
關閉保存 win.ini，重新啓動 Windows
del c:\msdos98.exe
del c:\windows\uninst~1.exe
del c:\windows\system\mine.exe
ＯＫ
60. MoSucker
清除木馬的步驟：

打開 system.ini 文件
查找到 shell=Explorer.exe unin0686.exe
更改爲：shell= Explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除 C:\windows\unin0686.exe
ＯＫ
61. Naebi v2.12 - 2.40
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\ICQ
v2.12 刪除右邊的專案：path= "C:\windows\msramgr.exe "
v2.15 刪除右邊的專案：path= "C:\windows\ msdll32.exe "
v2.19 刪除右邊的專案：path= "C:\windows\ naebi219.exe "
v2.xx 刪除右邊的專案：path= "C:\windows\ naebi219.exe "檔案名可能還是 naebi.exe , ns220.exe, ns227, ns231, ns234
關閉保存 Regedit
v2.34 和上面相同，但它在 win.ini 增加了啓動
打開 win.ini 文件
把 run=後面的路徑刪除
關閉保存 win.ini，重新啓動 Windows
查找相應的木馬程式，並刪除
ＯＫ
62. NetController v1.08
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：System = 'c:\windows\system.exe'
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\system.exe
ＯＫ
63. NetRaider v0.0
清除木馬的步驟：

打開註冊表 Regedit

點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Rsrcnrs = 'C:\windows\rsrcnrs.exe'
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\rsrcnrs.exe
ＯＫ
64. NetSphere v1.0 - 1.31337
清除木馬 v1.0-1.30：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：NSSX ="C:\WINDOWS\system\nssx.exe"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_USERS****\Software\Microsoft\Windows\CurrentVersion\Run
刪除專案同上。
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\system\nssx.exe
ＯＫ
清除木馬 v1.30-1.31337：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：ExecPowerProfile ="C:\WINDOWS\system\epp32.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\system\epp32.exe
ＯＫ
65. NetSpy v1.0 - 2.0
清除木馬 v1.0：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SysProtect = "c:\windows\system\system.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\system\system.exe
ＯＫ

清除木馬 v2.0：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Netspy = "netspy.exe"
關閉保存 Regedit，重新啓動 Windows
查找到 netspy.exe，並刪除
ＯＫ
66. NetTrojan v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：*** = "C:\WINDOWS\System\glide16.exe"
關閉保存 Regedit
打開 win.ini 文件
查找到 run=c:\windows\fxp.exe
把 run=後面的路徑刪除
關閉保存 win.ini，重新啓動 Windows
查找相應的木馬程式，並刪除
ＯＫ
67. Nirvana / VisualKiller v1.94 - 1.95
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：TheDoor = 'c:\windows\fonts\ariel.exe'
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\fonts\ariel.exe
ＯＫ
68. Phaze Zero v1.0b + 1.1
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：MsgServ = "msgsvr32.exe"
關閉保存 Regedit，重新啓動 Windows
查找相應的木馬程式，並刪除
ＯＫ
69. Prayer v1.2 - 1.5
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SysFiles = "C:\WINDOWS\System\dlls32.exe"
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SysFiles = "C:\WINDOWS\System\dlls32.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\System\dlls32.exe
ＯＫ
70. PRIORITY (Beta)
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Services
\
刪除右邊的專案："PServer"= C:\Windows\System\PServer.exe
關閉保存 Regedit，重新啓動 Windows
刪除 C:\Windows\System\PServer.exe
ＯＫ
71. Progenic Password Thief / Keylogger v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：pwt ="C:\WINDOWS\SYSTEM\pwt.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\SYSTEM\pwt.exe
ＯＫ

72. Progenic v1.0 -3.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Scandisk = "C:\WINDOWS\scandiskvr.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\scandiskvr.exe
ＯＫ
73. Prosiak beta - 0.70 b5
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
刪除右邊的專案：Microsoft DLL Loader = "windll32.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\ windll32.exe
ＯＫ
74. Retrieve v1.3
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Microsoft Access ="C:\WINDOWS\access.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\access.exe
ＯＫ
75. Revenger v1.0 - 1.5
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：AppName ="C:\...\server.exe"
關閉保存 Regedit，重新啓動 Windows

在 c:\windows 查找相應的木馬程式 server.exe，並刪除
ＯＫ
76. Ripper
清除木馬的步驟：

打開 system.ini 文件
將 shell=explorer.exe sysrunt.exe
改爲 shell= explorer.exe
關閉保存 system.ini，重新啓動 Windows
在 c:\windows 查找相應的木馬程式 sysrunt.exe，並刪除
ＯＫ
77. Satans Back Door v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
刪除右邊的專案：sysprot protection ="C:\windows\sysprot.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\sysprot.exe
ＯＫ
78. Schwindler v1.82
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：User.exe = "C:\WINDOWS\User.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\User.exe
ＯＫ
79. Setup Trojan (Sshare) +Mod Small Share
這個共用隱藏Ｃ盤的木馬
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\Lan

Man\
選擇右邊有'C$'的專案，並全部刪除
關閉保存 Regedit，重新啓動 Windows
ＯＫ
80. ShadowPhyre v2.12.38 - 2.X
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：WinZipp = "C:\WINDOWS\SYSTEM\WinZipp.exe /nomsg"
或者 WinZip = "C:\WINDOWS\SYSTEM\WinZip.exe /nomsg"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\ WinZipp.exe 或者 C:\WINDOWS\ WinZip.exe
ＯＫ
81. Share All

清除木馬的步驟：
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Network\LanMan\
這裏你將看到所有被木馬共用出來的你的硬碟符號，把它們一個個刪除掉。

82. ShitHeap
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
刪除右邊的專案：recycle-bin = "c:\windows\system\recycle-bin.exe"
或者 recycle-bin = "c:\windows\system.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\system\recycle-bin.exe 或者 c:\windows\system.exe
ＯＫ
83. Snid v1 - 2
清除木馬的步驟：

打開註冊表 Regedit

點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：System-tray = 'c:\windows\temp$01.exe'
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\temp$01.exe
ＯＫ
84. Softwarst
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：NetApp = C:\windows\system\winserv.exe
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\winserv.exe
ＯＫ
85. Spirit 2000 Beta - v1.2 (fixed)
清除木馬 v Beta 版本:

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：internet = "c:\windows\netip.exe "
關閉保存 Regedit
打開 win.ini 文件
查找到 run=c:\windows\netip.exe
更改爲：run=
關閉保存 win.ini，重新啓動 Windows
刪除 c:\windows\netip.exe 和 c:\windows\netip.exe
ＯＫ

清除木馬 v 1.2 版本:
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SystemTray = "c:\windows\windown.exe "
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\windown.exe

ＯＫ

清除木馬 v 1.2(fixed)版本:
打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Server 1.2.exe = "c:\windows\server 1.2.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\server 1.2.exe
ＯＫ
86. Stealth v2.0 - 2.16
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Winprotect System = "C:\WINDOWS\winprotecte.exe
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\winprotecte.exe
ＯＫ
87. SubSeven - Introduction
清除木馬 v1.0 - 1.1：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SystemTrayIcon = "C:\WINDOWS\SysTrayIcon.Exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\SysTrayIcon.Exe
ＯＫ

清除木馬 v1.3 - 1.4 - 1.5：

打開 win.ini 文件
查找到 run=nodll
更改爲 run=
關閉保存 win.ini，重新啓動 Windows
刪除 c:\windows\nodll.exe

ＯＫ

清除木馬 v1.6：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SystemTray = "SysTray.Exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\systray.exe
ＯＫ

清除木馬 v1.7：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
查找到右邊的專案：C:\windows\kernel16.dl，並刪除
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\kernel16.dl
ＯＫ

清除木馬 v1.8：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
查找到右邊的專案：c:\windows\system.ini.，並刪除
關閉保存 Regedit。
打開 win.ini 文件
查找到 run= kernel16.dl
更改爲 run=
關閉保存 win.ini。
打開 system.ini 文件
查找到 shell=explorer.exe kernel32.dl

更改爲 shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除 C:\windows\kernel16.dl
ＯＫ

清除木馬 v1.9 - 1.9b：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
刪除右邊的專案：RegistryScan = "rundll16.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\rundll16.exe
ＯＫ

清除木馬 v2.0：

打開 system.ini 文件
查找到 shell=explorer.exe trojanname.exe
更改爲 shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除 c:\windows\rundll16.exe
ＯＫ

清除木馬 v2.1 - 2.1 Gold + SubStealth- 2.1.3 Mod + 2.1.3 MUIE + 2.1 Bonus：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
\
刪除右邊的專案：WinLoader = MSREXE.EXE
hkey_classes_root\exefile\shell\open\command
將右邊的專案更改爲：@="\"%1\" %*"
關閉保存 Regedit。

打開 win.ini 文件
查找到 run=msrexe.exe 和
load=msrexe.exe
更改爲 run=
load=
關閉保存 win.ini。
打開 system.ini 文件
查找到 shell=explore.exe msrexe.exe
更改爲 shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除 C:\windows\ msrexe.exe
C:\windows\system\systray.dll
ＯＫ

清除木馬 v2.2b1：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和
刪除右邊的專案：載入器 = "c:\windows\system***"
注：載入器和檔案名是隨意改變的
關閉保存 Regedit。
打開 win.ini 文件
更改爲 run=
關閉保存 win.ini。
打開 system.ini 文件
更改爲 shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除相對應的木馬程式
ＯＫ

88. Telecommando 1.54
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SystemApp＝"ODBC.EXE"

關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\ ODBC.EXE
ＯＫ
89. The Unexplained
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：InetBOOst = "C:\WINDOWS\TEMPINETBOOST.EXE"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\TEMPINETBOOST.EXE
ＯＫ
90. Thing v1.00 - 1.60
清除木馬 v1.00-1.12：

點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：(Default) = "C:\some\path\here\thing.exe"
也有一些是在：
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\SessionManager\Known16D
LLs\
刪除右邊的專案：wsasrv.exe = "wsasrv.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\some\path\here\thing.exe
ＯＫ

清除木馬 v 1.20 版本:
進入 MS_DOS 方式：
del winspc13.exe
del ms097.exe
打開 system.ini 文件
查找到 shell=explorer.exe ms097.exe
更改爲：shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
ＯＫ

清除木馬 v1.50 版本:

點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
這個專案的路徑和檔案名是隨機改變的，察看有可疑的文件路徑，將它刪除。
關閉保存 Regedit。
打開 system.ini 文件
查找到 shell=explorer.exe 後面是木馬文件
更改爲：shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除相應的木馬文件
ＯＫ

清除木馬 v1.50 版本:
進入 MS_DOS 方式：
del winspc13.exe
del ms097.exe
打開 system.ini 文件
查找到 shell=explorer.exe 後面是木馬文件
更改爲：shell=explorer.exe
關閉保存 system.ini，重新啓動 Windows
刪除相應的木馬文件
ＯＫ
91. Transmission Scount v1.1 - 1.2
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Kernel16" = C:\WINDOWS\Kernel16.exe
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\Kernel16.exe
ＯＫ
92. Trinoo
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案： System Services = service.exe

關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\service.exe
ＯＫ
93. Trojan Cow v1.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SysWindow = "C:\WINDOWS\Syswindow.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\Syswindow.exe
ＯＫ
94. TryIt
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Rc5Dec = C:\Program Files\Internet Explorer_.exe -guistart
關閉保存 Regedit，重新啓動 Windows
刪除 C:\Program Files\Internet Explorer_.exe
ＯＫ
95. Vampire v1.0 - 1.2
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Sockets ="c:\windows\system\Sockets.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\windows\system\Sockets.exe
ＯＫ
96. WarTrojan v1.0 - 2.0
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：Kernel32 = "C:\somepath\server.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\somepath\server.exe
ＯＫ
97. wCrat v1.2b
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：MS Windows System Explorer ="C:\WINDOWS\sysexplor.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\sysexplor.exe
ＯＫ
98. WebEx (v1.2, 1.3, and 1.4)
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：RunDl32 = "C:\windows\system\task_bar"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\task_bar.exe 和 c:\windows\system\msinet.ocx
ＯＫ
99. WinCrash v2
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：WinManager = "c:\windows\server.exe"
關閉保存 Regedit
打開 win.ini 文件
查找到 run=c:\windows\server.exe
更改爲：run=
保存關閉 win.ini，重新啓動 Windows
刪除 c:\windows\server.exe

ＯＫ
100. WinCrash
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：MsManager ="SERVER.EXE"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\windows\system\ SERVER.EXE
ＯＫ
101. Xanadu v1.1
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：SETUP = "c:\somepath\setup.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 c:\somepath\setup.exe
ＯＫ
102. Xplorer v1.20
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：PCX = "C:\WINDOWS\system\PCX.exe"
關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\system\PCX.exe
ＯＫ
103. Xtcp v2.0 - 2.1
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
刪除右邊的專案：msgsv32 = "C:\WINDOWS\system\winmsg32.exe"

關閉保存 Regedit，重新啓動 Windows
刪除 C:\WINDOWS\system\winmsg32.exe
ＯＫ
104. YAT
清除木馬的步驟：

打開註冊表 Regedit
點擊目錄至：
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
刪除右邊的專案：Batterieanzeige = 'c:\pathnamehere\server.exe /nomsg'
關閉保存 Regedit，重新啓動 Windows
刪除 c:\pathnamehere\server.exe
ＯＫ