

# Re: hijack this startup – can someone tell me the hack i am experienci

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2005-01/2309.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-01/2309.html)

---

**From:** Carey Frisch [MVP] ([cnfrisch\\_at\\_nospamgmail.com](mailto:cnfrisch_at_nospamgmail.com))

**Date:** 01/28/05

Date: Thu, 27 Jan 2005 18:03:23 -0600

I don't think anyone has the time to analyse your lengthy  
"Hijack This" log (a non-Microsoft supported program).  
I would suggest you perform the following:

Symantec Security Check

<http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym>

3 Simple Steps to Help Ensure the Protection of Your PC

<http://www.microsoft.com/athome/security/protect/default.aspx>

Microsoft Windows AntiSpyware

<http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&displaylan>

--  
Carey Frisch  
Microsoft MVP  
Windows XP - Shell/User  
Be Smart! Protect Your PC!  
<http://www.microsoft.com/athome/security/protect/default.aspx>

-----  
"Pfused\_the\_Confused" wrote:

| this is a Hijack This startup log - as you can see, i am being hacked but i  
| don't know how to interpret all the data. i believe they created a hidden  
| partition on my drive, have taken over admin rights and are impersonating the  
| one user (vince) on the machine.

| any help would be most appreciated!!!

| sorry for posting such a large log file - the remainder is in a second post  
| with the same title

| (config = winxp sp2 all updates - panasonic touchbook elite - broadband  
| access through shaw internet)

| StartupList report, 1/27/2005, 3:33:50 PM  
| StartupList version: 1.52.2  
| Started from : C:\Program Files\hijack tmp\HijackThis.EXE  
| Detected: Windows XP SP2 (WinNT 5.01.2600)  
| Detected: Internet Explorer v6.00 SP2 (6.00.2900.2180)  
| \* Using default options

```
* Including empty and uninteresting sections
* Showing rarely important sections
=====

Running processes:

C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe
C:\WINDOWS\Explorer.EXE
C:\Program Files\Common Files\Symantec Shared\ccEvtMgr.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\Symantec AntiVirus\DefWatch.exe
C:\Program Files\Symantec AntiVirus\Rtvscan.exe
C:\Program Files\UPHClean\uphclean.exe
C:\Program Files\Common Files\Symantec Shared\ccApp.exe
C:\PROGRA~1\SYMANT~1\VPTray.exe
C:\WINDOWS\system32\igfxtray.exe
C:\WINDOWS\system32\hkcmd.exe
C:\WINDOWS\system32\hkeyman.exe
C:\Program Files\QuickTime\qttask.exe
C:\PROGRA~1\Mizotec\xpnsbar.exe
C:\Program Files\WinZip\WZQKPICK.EXE
C:\WINDOWS\system32\mmc.exe
C:\WINDOWS\PCHealth\HelpCtr\Binaries\HelpCtr.exe
C:\WINDOWS\PCHealth\HelpCtr\Binaries\HelpSvc.exe
C:\WINDOWS\PCHealth\HelpCtr\Binaries\HelpHost.exe
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\WINDOWS\system32\rundll32.exe
C:\Program Files\hijack tmp\HijackThis.exe
C:\WINDOWS\system32\notepad.EXE
C:\WINDOWS\system32\taskmgr.exe
C:\WINDOWS\notepad.exe

-----

Listing of startup folders:

Shell folders Startup:
[C:\Documents and Settings\Vince\Start Menu\Programs\Startup]
*No files*

Shell folders AltStartup:
*Folder not found*

User shell folders Startup:
*Folder not found*

User shell folders AltStartup:
*Folder not found*

Shell folders Common Startup:
[C:\Documents and Settings\All Users\Start Menu\Programs\Startup]
Adobe Reader Speed Launch.lnk = C:\Program Files\Adobe\Acrobat
7.0\Reader\reader_sl.exe
WinZip Quick Pick.lnk = C:\Program Files\WinZip\WZQKPICK.EXE
```

```
| Shell folders Common AltStartup:  
| *Folder not found*  
  
| User shell folders Common Startup:  
| *Folder not found*  
  
| User shell folders Alternate Common Startup:  
| *Folder not found*  
  
|-----  
  
| Checking Windows NT UserInit:  
  
| [HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]  
| UserInit = C:\WINDOWS\system32\userinit.exe,  
  
| [HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon]  
| *Registry key not found*  
  
| [HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]  
| *Registry value not found*  
  
| [HKCU\Software\Microsoft\Windows\CurrentVersion\Winlogon]  
| *Registry key not found*  
  
|-----  
  
| Autorun entries from Registry:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
  
| ccApp = "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"  
| vptray = C:\PROGRA~1\SYMAN~1\VPTray.exe  
| PCTVOICE = pctspk.exe  
| IgfxTray = C:\WINDOWS\system32\igfxtray.exe  
| HotKeysCmds = C:\WINDOWS\system32\hkcmd.exe  
| Hotkey = C:\WINDOWS\system32\hkeyman.exe  
| QuickTime Task = "C:\Program Files\QuickTime\qttask.exe" -atboottime  
| Mizo - XP Netstats Bar = C:\PROGRA~1\Mizotec\xpnsbar.exe  
  
|-----  
  
| Autorun entries from Registry:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
  
| *No values found*  
  
|-----  
  
| Autorun entries from Registry:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx  
  
| *No values found*  
  
|-----  
  
| Autorun entries from Registry:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices  
  
| *Registry key not found*  
  
|-----
```

microsoft.public.windowsxp.security\_admin: Re: hijack this startup – can someone tell me the hack i am experienci

```
Autorun entries from Registry:
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
*Registry key not found*
-----

Autorun entries from Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
*No values found*
-----

Autorun entries from Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
*Registry key not found*
-----

Autorun entries from Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
*Registry key not found*
-----

Autorun entries from Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
*Registry key not found*
-----

Autorun entries from Registry:
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
*Registry key not found*
-----

Autorun entries from Registry:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Run
*Registry key not found*
-----

Autorun entries from Registry:
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Run
*Registry key not found*
-----

Autorun entries in Registry subkeys of:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
*No subkeys found*
-----
```

Re: hijack this startup – can someone tell me the hack i am experienci

```
| Autorun entries in Registry subkeys of:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce  
| *No subkeys found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx  
| *No subkeys found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
| *No subkeys found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Run  
| *Registry key not found*  
|-----  
| Autorun entries in Registry subkeys of:  
| HKCU\Software\Microsoft\Windows NT\CurrentVersion\Run
```

```
*Registry key not found*
-----

File association entry for .EXE:
HKEY_CLASSES_ROOT\exefile\shell\open\command

(Default) = "%1" %*
-----

File association entry for .COM:
HKEY_CLASSES_ROOT\comfile\shell\open\command

(Default) = "%1" %*
-----

File association entry for .BAT:
HKEY_CLASSES_ROOT\batfile\shell\open\command

(Default) = "%1" %*
-----

File association entry for .PIF:
HKEY_CLASSES_ROOT\piffile\shell\open\command

(Default) = "%1" %*
-----

File association entry for .SCR:
HKEY_CLASSES_ROOT\scrfile\shell\open\command

(Default) = "%1" /S
-----

File association entry for .HTA:
HKEY_CLASSES_ROOT\htafile\shell\open\command

(Default) = C:\WINDOWS\System32\mshta.exe "%1" %*
-----

File association entry for .TXT:
HKEY_CLASSES_ROOT\txtfile\shell\open\command

(Default) = %SystemRoot%\system32\notepad.exe %1
-----

Enumerating Active Setup stub paths:
HKLM\Software\Microsoft\Active Setup\Installed Components
(* = disabled by HKCU twin)

[>{22d6f312-b0f6-11d0-94ab-0080c74c7e95}]
StubPath = C:\WINDOWS\inf\unregmp2.exe /ShowWMP

[>{26923b43-4d38-484f-9b9e-de460746276c}] *
StubPath = %systemroot%\system32\shmgrate.exe OCInstallUserConfigIE
```

```
[>{60B49E34-C7CC-11D0-8953-00A0C90347FF}MICROS] *
StubPath = RunDLL32 IEDKCS32.DLL,BrandIE4 SIGNUP

[>{881dd1c5-3dcf-431b-b061-f3f88e8be88a}] *
StubPath = %systemroot%\system32\shmgrate.exe OCInstallUserConfigOE

[{2C7339CF-2B09-4501-B3F3-F3508C9228ED}] *
StubPath = %SystemRoot%\system32\regsvr32.exe /s /n /i:/UserInstall
%SystemRoot%\system32\themeui.dll

[{44BBA840-CC51-11CF-AAFA-00AA00B6015C}] *
StubPath = "%ProgramFiles%\Outlook Express\setup50.exe" /APP:OE
/CALLER:WINNT /user /install

[{44BBA842-CC51-11CF-AAFA-00AA00B6015B}] *
StubPath = rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\msnetmtg.inf,NetMtg.Install.PerUser.NT

[{4b218e3e-bc98-4770-93d3-2731b9329278}] *
StubPath = %SystemRoot%\System32\rundll32.exe setupapi,InstallHinfSection
MarketplaceLinkInstall 896 %systemroot%\inf\ie.inf

[{5945c046-1e7d-11d1-bc44-00c04fd912be}] *
StubPath = rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\msmsgs.inf,BLC.QuietInstall.PerUser

[{6BF52A52-394A-11d3-B153-00C04F79FAA6}] *
StubPath = rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\wmp.inf,PerUserStub

[{7790769C-0471-11d2-AF11-00C04FA35D02}] *
StubPath = "%ProgramFiles%\Outlook Express\setup50.exe" /APP:WAB
/CALLER:WINNT /user /install

[{89820200-ECBD-11cf-8B85-00AA005B4340}] *
StubPath = regsvr32.exe /s /n /i:U shell32.dll

[{89820200-ECBD-11cf-8B85-00AA005B4383}] *
StubPath = %SystemRoot%\system32\ie4uunit.exe

-----

Enumerating ICQ Agent Autostart apps:
HKCU\Software\Mirabilis\ICQ\Agent\Apps

*Registry key not found*

-----

Load/Run keys from C:\WINDOWS\WIN.INI:

load=*INI section not found*
run=*INI section not found*

Load/Run keys from Registry:

HKLM\..\Windows NT\CurrentVersion\WinLogon: load=*Registry value not found*
HKLM\..\Windows NT\CurrentVersion\WinLogon: run=*Registry value not found*
HKLM\..\Windows\CurrentVersion\WinLogon: load=*Registry key not found*
HKLM\..\Windows\CurrentVersion\WinLogon: run=*Registry key not found*
HKCU\..\Windows NT\CurrentVersion\WinLogon: load=*Registry value not found*
```

```
| HKCU\..\Windows NT\CurrentVersion\WinLogon: run=*Registry value not found*  
| HKCU\..\Windows\CurrentVersion\WinLogon: load=*Registry key not found*  
| HKCU\..\Windows\CurrentVersion\WinLogon: run=*Registry key not found*  
| HKCU\..\Windows NT\CurrentVersion\Windows: load=  
| HKCU\..\Windows NT\CurrentVersion\Windows: run=*Registry value not found*  
| HKLM\..\Windows NT\CurrentVersion\Windows: load=*Registry value not found*  
| HKLM\..\Windows NT\CurrentVersion\Windows: run=*Registry value not found*  
| HKLM\..\Windows NT\CurrentVersion\Windows: AppInit_DLLs=
```

-----  
Shell & screensaver key from C:\WINDOWS\SYSTEM.INI:

```
Shell=*INI section not found*  
SCRNSAVE.EXE=*INI section not found*  
drivers=*INI section not found*
```

Shell & screensaver key from Registry:

```
Shell=Explorer.exe  
SCRNSAVE.EXE=  
drivers=*Registry value not found*
```

Policies Shell key:

```
HKCU\..\Policies: Shell=*Registry key not found*  
HKLM\..\Policies: Shell=*Registry value not found*
```

-----  
Checking for EXPLORER.EXE instances:

```
C:\WINDOWS\Explorer.exe: PRESENT!  
  
C:\Explorer.exe: not present  
C:\WINDOWS\Explorer\Explorer.exe: not present  
C:\WINDOWS\System\Explorer.exe: not present  
C:\WINDOWS\System32\Explorer.exe: not present  
C:\WINDOWS\Command\Explorer.exe: not present  
C:\WINDOWS\Fonts\Explorer.exe: not present
```

-----  
Checking for superhidden extensions:

```
.lnk: HIDDEN! (arrow overlay: yes)  
.pif: HIDDEN! (arrow overlay: yes)  
.exe: not hidden  
.com: not hidden  
.bat: not hidden  
.hta: not hidden  
.scr: not hidden  
.shs: HIDDEN!  
.shb: HIDDEN!  
.vbs: not hidden  
.vbe: not hidden  
.wsh: not hidden  
.scf: HIDDEN! (arrow overlay: NO!)  
.url: HIDDEN! (arrow overlay: yes)  
.js: not hidden  
.jse: not hidden
```

```
-----  
Verifying REGEDIT.EXE integrity:  
  
- Regedit.exe found in C:\WINDOWS  
- .reg open command is normal (regedit.exe %1)  
- Company name OK: 'Microsoft Corporation'  
- Original filename OK: 'REGEDIT.EXE'  
- File description: 'Registry Editor'  
  
Registry check passed  
  
-----  
Enumerating Browser Helper Objects:  
  
(no name) - C:\Program Files\Adobe\Acrobat 7.0\ActiveX\AcroIEHelper.dll -  
{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}  
  
-----  
Enumerating Task Scheduler jobs:  
  
*No jobs found*  
  
-----  
Enumerating Download Program Files:  
  
[Office Update Installation Engine]  
InProcServer32 = C:\WINDOWS\opuc.dll  
CODEBASE = http://office.microsoft.com/officeupdate/content/opuc.cab  
  
[Shockwave Flash Object]  
InProcServer32 = C:\WINDOWS\system32\macromed\flash\Flash.ocx  
CODEBASE = http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab  
  
[MSN Money Ticker]  
InProcServer32 = C:\WINDOWS\Downloaded Program Files\ticker13.ocx  
CODEBASE = http://fdl.msn.com/public/investor/v13/ticker.cab  
  
-----  
Enumerating Winsock LSP files:  
  
NameSpace #1: C:\WINDOWS\System32\mswsock.dll  
NameSpace #2: C:\WINDOWS\System32\winrnr.dll  
NameSpace #3: C:\WINDOWS\System32\mswsock.dll  
Protocol #1: C:\WINDOWS\system32\mswsock.dll  
Protocol #2: C:\WINDOWS\system32\mswsock.dll  
Protocol #3: C:\WINDOWS\system32\mswsock.dll  
Protocol #4: C:\WINDOWS\system32\rsvpsp.dll  
Protocol #5: C:\WINDOWS\system32\rsvpsp.dll  
Protocol #6: C:\WINDOWS\system32\mswsock.dll  
Protocol #7: C:\WINDOWS\system32\mswsock.dll  
Protocol #8: C:\WINDOWS\system32\mswsock.dll  
Protocol #9: C:\WINDOWS\system32\mswsock.dll  
Protocol #10: C:\WINDOWS\system32\mswsock.dll  
Protocol #11: C:\WINDOWS\system32\mswsock.dll  
  
-----
```

```
| Enumerating Windows NT/2000/XP services
|
| Intel(r) 82801 Audio Driver Install Service (WDM):
| system32\drivers\ac97intc.sys (manual start)
| Microsoft ACPI Driver: System32\DRIVERS\ACPI.sys (system)
| Microsoft Embedded Controller Driver: System32\DRIVERS\ACPIEC.sys (system)
| Microsoft Kernel Acoustic Echo Cancellor: system32\drivers\aec.sys (manual
| start)
| AFD Networking Support Environment: \SystemRoot\System32\drivers\afd.sys
| (system)
| Alerter: %SystemRoot%\System32\svchost.exe -k LocalService (disabled)
| Application Layer Gateway Service: %SystemRoot%\System32\alg.exe (manual
| start)
| Application Management: %SystemRoot%\system32\svchost.exe -k netsvcs (manual
| start)
| RAS Asynchronous Media Driver: System32\DRIVERS\asynmac.sys (manual start)
| Standard IDE/ESDI Hard Disk Controller: System32\DRIVERS\atapi.sys (system)
| ATM ARP Client Protocol: System32\DRIVERS\atmarpc.sys (manual start)
| Windows Audio: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Audio Stub Driver: System32\DRIVERS\audstub.sys (manual start)
| Background Intelligent Transfer Service: %SystemRoot%\System32\svchost.exe
| -k netsvcs (manual start)
| Computer Browser: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Symantec Event Manager: "C:\Program Files\Common Files\Symantec
| Shared\ccEvtMgr.exe" (autostart)
| Symantec Password Validation: "C:\Program Files\Common Files\Symantec
| Shared\ccPwdSvc.exe" (manual start)
| Symantec Settings Manager: "C:\Program Files\Common Files\Symantec
| Shared\ccSetMgr.exe" (autostart)
| CD-ROM Driver: System32\DRIVERS\cdrom.sys (system)
| Indexing Service: %SystemRoot%\system32\cisvc.exe (manual start)
| ClipBook: %SystemRoot%\system32\clipsrv.exe (disabled)
| Microsoft ACPI Control Method Battery Driver: System32\DRIVERS\CmBatt.sys
| (manual start)
| Microsoft Composite Battery Driver: System32\DRIVERS\compbatt.sys (system)
| COM+ System Application: C:\WINDOWS\System32\dlhhost.exe
| /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235} (manual start)
| Cryptographic Services: %SystemRoot%\system32\svchost.exe -k netsvcs
| (autostart)
| DCOM Server Process Launcher: %SystemRoot%\system32\svchost -k DcomLaunch
| (autostart)
| Symantec AntiVirus Definition Watcher: "C:\Program Files\Symantec
| AntiVirus\DefWatch.exe" (autostart)
| DHCP Client: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Disk Driver: System32\DRIVERS\disk.sys (system)
| Logical Disk Manager Administrative Service:
| %SystemRoot%\System32\dmadmin.exe /com (manual start)
| dmboot: System32\drivers\dmboot.sys (disabled)
| Logical Disk Manager Driver: System32\drivers\dmio.sys (system)
| dmload: System32\drivers\dmload.sys (system)
| Logical Disk Manager: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Microsoft Kernel DLS Syntheiszer: system32\drivers\DMusic.sys (manual start)
| DNS Client: %SystemRoot%\System32\svchost.exe -k NetworkService (autostart)
| Microsoft Kernel DRM Audio Descrambler: system32\drivers\drmkaud.sys (manual
| start)
| Error Reporting Service: %SystemRoot%\System32\svchost.exe -k netsvcs
| (autostart)
| Event Log: %SystemRoot%\system32\services.exe (autostart)
| COM+ Event System: C:\WINDOWS\System32\svchost.exe -k netsvcs (manual start)
| Fast User Switching Compatibility: %SystemRoot%\System32\svchost.exe -k
| netsvcs (manual start)
| FltMgr: system32\drivers\fltMgr.sys (system)
```

```
| Volume Manager Driver: System32\DRIVERS\ftdisk.sys (system)
| Generic Packet Classifier: System32\DRIVERS\msgpc.sys (manual start)
| Help and Support: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Human Interface Device Access: %SystemRoot%\System32\svchost.exe -k netsvcs
| (disabled)
| Panasonic Hotkey Driver: system32\DRIVERS\HOTKEY.SYS (manual start)
| HTTP: System32\Drivers\HTTP.sys (manual start)
| HTTP SSL: %SystemRoot%\System32\svchost.exe -k HTTPFilter (manual start)
| i8042 Keyboard and PS/2 Mouse Port Driver: System32\DRIVERS\i8042prt.sys
| (system)
| ialm: system32\DRIVERS\ialmnt5.sys (manual start)
| CD-Burning Filter Driver: System32\DRIVERS\imapi.sys (system)
| IMAPI CD-Burning COM Service: C:\WINDOWS\System32\imapi.exe (manual start)
| IntelIde: System32\DRIVERS\intelide.sys (system)
| Intel Processor Driver: System32\DRIVERS\intelppm.sys (system)
| IPv6 Windows Firewall Driver: system32\drivers\ip6fw.sys (manual start)
| IP Traffic Filter Driver: System32\DRIVERS\ipfltdrv.sys (manual start)
| IP in IP Tunnel Driver: System32\DRIVERS\ipinip.sys (manual start)
| IP Network Address Translator: System32\DRIVERS\ipnat.sys (manual start)
| IPSEC driver: System32\DRIVERS\ipsec.sys (system)
| IR Enumerator Service: System32\DRIVERS\irenum.sys (manual start)
| PnP ISA/EISA Bus Driver: System32\DRIVERS\isapnp.sys (system)
| Keyboard Class Driver: System32\DRIVERS\kbdclass.sys (system)
| Microsoft Kernel Wave Audio Mixer: system32\drivers\kmixer.sys (manual start)
| Server: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Workstation: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| TCP/IP NetBIOS Helper: %SystemRoot%\System32\svchost.exe -k LocalService
| (autostart)
| Messenger: %SystemRoot%\System32\svchost.exe -k netsvcs (disabled)
| NetMeeting Remote Desktop Sharing: C:\WINDOWS\System32\mnmsrvc.exe (manual
| start)
| Mouse Class Driver: System32\DRIVERS\mouclass.sys (system)
| WebDav Client Redirector: System32\DRIVERS\mrxdav.sys (manual start)
| MRXSMB: System32\DRIVERS\mrxsmb.sys (system)
| Distributed Transaction Coordinator: C:\WINDOWS\System32\msdtc.exe (manual
| start)
| Windows Installer: C:\WINDOWS\System32\msiexec.exe /V (manual start)
| Microsoft Streaming Service Proxy: system32\drivers\MSKSSRV.sys (manual start)
| Microsoft Streaming Clock Proxy: system32\drivers\MSPCLOCK.sys (manual start)
| Microsoft Streaming Quality Manager Proxy: system32\drivers\MSPQM.sys
| (manual start)
| Microsoft System Management BIOS Driver: System32\DRIVERS\mssmbios.sys
| (manual start)
| NAVENG: \??\C:\PROGRA~1\COMMON~1\SYMANT~1\VIRUSD~1\20050119.041\naveng.sys
| (manual start)
| NAVEX15: \??\C:\PROGRA~1\COMMON~1\SYMANT~1\VIRUSD~1\20050119.041\navex15.sys
| (manual start)
| Remote Access NDIS TAPI Driver: System32\DRIVERS\ndistapi.sys (manual start)
| NDIS Usermode I/O Protocol: System32\DRIVERS\ndisuio.sys (manual start)
| Remote Access NDIS WAN Driver: System32\DRIVERS\ndiswan.sys (manual start)
| NetBIOS Interface: System32\DRIVERS\netbios.sys (system)
| NetBios over Tcpi: System32\DRIVERS\netbt.sys (system)
| Network DDE: %SystemRoot%\system32\netdde.exe (disabled)
| Network DDE DSDM: %SystemRoot%\system32\netdde.exe (disabled)
| Net Logon: %SystemRoot%\System32\lsass.exe (manual start)
| Network Connections: %SystemRoot%\System32\svchost.exe -k netsvcs (manual
| start)
| Network Location Awareness (NLA): %SystemRoot%\System32\svchost.exe -k
| netsvcs (manual start)
| NT LM Security Support Provider: %SystemRoot%\System32\lsass.exe (manual
| start)
| Removable Storage: %SystemRoot%\system32\svchost.exe -k netsvcs (manual start)
```

```
| IPX Traffic Filter Driver: System32\DRIVERS\nwlnkflt.sys (manual start)
| IPX Traffic Forwarder Driver: System32\DRIVERS\nwlnk fwd.sys (manual start)
| PCI Bus Driver: System32\DRIVERS\pci.sys (system)
| PCIId: system32\DRIVERS\pciide.sys (system)
| Pcmcia: System32\DRIVERS\pcmcia.sys (system)
| Plug and Play: %SystemRoot%\system32\services.exe (autostart)
| IPSEC Services: %SystemRoot%\System32\lsass.exe (autostart)
| WAN Miniport (PPTP): System32\DRIVERS\raspptp.sys (manual start)
| Processor Driver: System32\DRIVERS\processr.sys (system)
| Protected Storage: %SystemRoot%\system32\lsass.exe (autostart)
| QoS Packet Scheduler: System32\DRIVERS\psched.sys (manual start)
| Direct Parallel Link Driver: System32\DRIVERS\ptilink.sys (manual start)
| W2K Pctel Serial Device Driver: system32\DRIVERS\ptserial.sys (manual start)
| Remote Access Auto Connection Driver: System32\DRIVERS\rasacd.sys (system)
| Remote Access Auto Connection Manager: %SystemRoot%\System32\svchost.exe -k
| netsvcs (manual start)
| WAN Miniport (L2TP): System32\DRIVERS\rasl2tp.sys (manual start)
| Remote Access Connection Manager: %SystemRoot%\System32\svchost.exe -k
| netsvcs (manual start)
| Remote Access PPPOE Driver: System32\DRIVERS\rasppoe.sys (manual start)
| Direct Parallel: System32\DRIVERS\raspti.sys (manual start)
| Rdbss: System32\DRIVERS\rdbss.sys (system)
| RDP CDD: System32\DRIVERS\RDPCDD.sys (system)
| Terminal Server Device Redirector Driver: System32\DRIVERS\rdpdr.sys (manual
| start)
| Remote Desktop Help Session Manager: C:\WINDOWS\system32\sessmgr.exe (manual
| start)
| Digital CD Audio Playback Filter Driver: System32\DRIVERS\redbook.sys (system)
| Routing and Remote Access: %SystemRoot%\System32\svchost.exe -k netsvcs
| (disabled)
| Remote Registry: %SystemRoot%\system32\svchost.exe -k LocalService (autostart)
| Remote Procedure Call (RPC) Locator: %SystemRoot%\System32\locator.exe
| (manual start)
| Remote Procedure Call (RPC): %SystemRoot%\system32\svchost -k rpcss
| (autostart)
| QoS RSVP: %SystemRoot%\System32\rsvp.exe (manual start)
| Realtek RTL8139(A/B/C)-based PCI Fast Ethernet Adapter NT Driver:
| System32\DRIVERS\RTL8139.SYS (manual start)
| Security Accounts Manager: %SystemRoot%\system32\lsass.exe (autostart)
| SAVRoam: "C:\Program Files\Symantec AntiVirus\SavRoam.exe" (manual start)
| SAVRT: \??\C:\Program Files\Symantec AntiVirus\savrt.sys (system)
| SAVRTPEL: \??\C:\Program Files\Symantec AntiVirus\Savrtpel.sys (autostart)
| Smart Card: %SystemRoot%\System32\SCardSvr.exe (manual start)
| Task Scheduler: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Ricoh SD Bus Host Adapter : System32\Drivers\sdbus.sys (manual start)
| Memory Card: System32\Drivers\sdstmem.sys (manual start)
| Secdrv: System32\DRIVERS\secdrv.sys (manual start)
| Secondary Logon: %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| System Event Notification: %SystemRoot%\system32\svchost.exe -k netsvcs
| (autostart)
| Windows Firewall/Internet Connection Sharing (ICS):
| %SystemRoot%\System32\svchost.exe -k netsvcs (autostart)
| Shell Hardware Detection: %SystemRoot%\System32\svchost.exe -k netsvcs
| (autostart)
| Symantec Network Drivers Service: "C:\Program Files\Common Files\Symantec
| Shared\SNDSrv.exe" (manual start)
| Microsoft Kernel Audio Splitter: system32\drivers\splitter.sys (manual start)
| Print Spooler: %SystemRoot%\system32\spoolsv.exe (autostart)
| System Restore Filter Driver: \SystemRoot\System32\DRIVERS\sr.sys (disabled)
| System Restore Service: %SystemRoot%\System32\svchost.exe -k netsvcs
| (autostart)
| Srv: System32\DRIVERS\srv.sys (manual start)
```

microsoft.public.windowsxp.security\_admin: Re: hijack this startup – can someone tell me the hack i am experienci

```
| SSDP Discovery Service: %SystemRoot%\System32\svchost.exe -k LocalService
| (manual start)
| Windows Image Acquisition (WIA): %SystemRoot%\System32\svchost.exe -k imgsvc
| (manual start)
| Software Bus Driver: System32\DRIVERS\swenum.sys (manual start)
| Microsoft Kernel GS Wavetable Synthesizer: system32\drivers\swmidi.sys
| (manual start)
| MS Software Shadow Copy Provider: C:\WINDOWS\System32\dllhost.exe
| /Processid:{D00B1DD8-F5AF-4905-ABB3-3830CB984851} (manual start)
| Symantec AntiVirus: "C:\Program Files\Symantec AntiVirus\Rtvscan.exe"
| (autostart)
| SymEvent: \??\C:\Program Files\Symantec\SYMEVENT.SYS (manual start)
| SYMREDRV: \SystemRoot\System32\Drivers\SYMREDRV.SYS (manual start)
| SYMTDI: \SystemRoot\System32\Drivers\SYMTDI.SYS (system)
| Microsoft Kernel System Audio Device: system32\drivers\sysaudio.sys (manual
| start)
| Performance Logs and Alerts: %SystemRoot%\system32\smlogsvc.exe (manual start)
| Telephony: %SystemRoot%\System32\svchost.exe -k netsvcs (manual start)
| TCP/IP Protocol Driver: System32\DRIVERS\tcpip.sys (system)
| Terminal Device Driver: System32\DRIVERS\termdd.sys (system)
| Terminal Services: %SystemRoot%\System32\svchost -k DComLaunch (manual start)
```