

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

IRC Packets being generated. Dont know where from...

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-04/0389.html>

From: Scooter (*scott_at_serra.com*)

Date: 04/27/05

Date: 26 Apr 2005 15:07:46 -0700

I have a PC that is generating IRC Query packets on our network.
I've turned off all the services it will let me and its still there.
If I boot into Safe mode it does not send the packets.
I've included a copy of the Packet and a HiJackThis Log...

HELP!

Thanks!

Copy of the packet Decoded by EtherPeek:

Packet Info

Flags: 0x00

Status: 0x00

Packet Length: 96

Timestamp: 14:51:34.685357 04/26/2005

Ethernet Header

Destination: FF:FF:FF:FF:FF:FF Ethernet Broadcast

Source: 00:48:54:3B:69:12 [PHY]

Protocol Type: 0x0800 IP

IP Header – Internet Protocol Datagram

Version: 4

Header Length: 5 (20 bytes)

Type of Service: %00000000

000. Precedence: Routine

...0 Normal Delay

.... 0... Normal Throughput

.... .0.. Normal Reliability

.... ..0. ECT bit – transport protocol will

ignore the CE bit

.... ...0 CE bit – no congestion

Total Length: 78

Identifier: 7469

Fragmentation Flags: %000

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

0.. Reserved
.0. May Fragment
..0 Last Fragment

Fragment Offset: 0 (0 bytes)
Time To Live: 128
Protocol: 17 UDP – User Datagram Protocol
Header Checksum: 0x0657
Source IP Address: 10.1.3.26
Dest. IP Address: 10.1.255.255
No IP Options
UDP – User Datagram Protocol
Source Port: 137 netbios–ns
Destination Port: 137 netbios–ns
Length: 58
Checksum: 0xD2AD
NetBIOS Name Service – Network Basic Input/Output System
Identification: 0xA133
Flags: 0x0110
0... .. Request
.000 0... .. Standard Query
... .0.. .. (Non–Authoritative answer)
... ..0. (Message Not Truncated)
... ..1 Recursion Desired
... .. 0... .. (Recursion Not Available)
... .. .0.. .. (Unknown Flag Off)
...0. (Unknown Flag Off)
...1 Packet Was Broadcast

Questions: 1
Answers: 0
Authority: 0
Additional: 0

Question

Domain Name: IRC.*.* <00> Workstation
Type: 32 NetBIOS General Name Service
Class: 1 Internet

FCS – Frame Check Sequence
FCS (Calculated): 0x65DF9921

HiJackThis Log

StartupList report, 4/26/2005, 2:46:19 PM
StartupList version: 1.52
Started from : F:\Spyware\HiJackThis\HijackThis.EXE
Detected: Windows 2000 SP4 (WinNT 5.00.2195)
Detected: Internet Explorer v6.00 SP1 (6.00.2800.1106)
* Using default options
* Including empty and uninteresting sections

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

* Showing rarely important sections

=====
Running processes:

C:\WINNT\System32\smss.exe
C:\WINNT\system32\winlogon.exe
C:\WINNT\system32\services.exe
C:\WINNT\system32\lsass.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\System32\svchost.exe
C:\WINNT\Explorer.EXE
C:\WINNT\system32\taskmgr.exe
C:\WINNT\REGEDIT.exe
C:\Program Files\Internet Explorer\IEXPLORE.EXE
C:\WINNT\system32\CMD.exe
F:\Spyware\HiJackThis\HijackThis.exe
C:\WINNT\system32\mmc.exe

Listing of startup folders:

Shell folders Startup:

[C:\Documents and Settings\Scott Townsend\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]

HP OfficeJet Series 700 Startup.lnk = C:\Program
Files\Hewlett-Packard\HP OfficeJet Series 700 NT\Bin\HPOstr05.exe

Microsoft Office.lnk = C:\Program Files\Microsoft
Office\Office10\OSA.EXE

VPN Client.lnk = C:\Program Files\Cisco Systems\VPN Client\vpngui.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

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

User shell folders Alternate Common Startup:

Folder not found

Checking Windows NT UserInit:

[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
UserInit = C:\WINNT\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

Synchronization Manager = mobsync.exe /logon

OfficeScanNT Monitor = "C:\Program Files\OfficeScan NT\pccntmon.exe"
-HideWindow

RealTray = C:\Program Files\Real\RealPlayer\RealPlay.exe

SYSTEMBOOTHIDEPLAYER

NeroCheck = C:\WINNT\system32\NeroCheck.exe

gcasServ = "C:\Program Files\Microsoft AntiSpyware\gcasServ.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

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

No values found

Autorun entries from Registry:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

Registry key not found

Autorun entries from Registry:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

ctfmon.exe = ctfmon.exe

Autorun entries from Registry:

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

No values 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

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

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

[OptionalComponents]

No values found

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

No subkeys 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

No subkeys found

IRC Packets being generated. Dont know where from...

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" %*

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

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:\WINNT\System32\mshta.exe "%1" %*

Enumerating Active Setup stub paths:

HKLM\Software\Microsoft\Active Setup\Installed Components

(* = disabled by HKCU twin)

[>{26923b43-4d38-484f-9b9e-de460746276c}] *

StubPath = "C:\WINNT\system32\shmgrate.exe" OCInstallUserConfigIE

[>{60B49E34-C7CC-11D0-8953-00A0C90347FF}MICROS] *

StubPath = RunDLL32 IEDKCS32.DLL,BrandIE4 SIGNUP

[>{881dd1c5-3dcf-431b-b061-f3f88e8be88a}] *

StubPath = "C:\WINNT\system32\shmgrate.exe" OCInstallUserConfigOE

[{22d6f312-b0f6-11d0-94ab-0080c74c7e95}] *

StubPath = rundll32.exe advpack.dll,LaunchINFSection

C:\WINNT\INF\mplayer2.inf,PerUserStub.NT

[{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:\WINNT\INF\msnetmtg.inf,NetMtg.Install.PerUser.NT

[{6A5110B5-E14B-4268-A065-EF89FF33C325}] *

StubPath = regsvr32.exe /s /n /i:"S 2 true 3 true 4 true 5 true 6 true

7 true" initpki.dll

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

```
[{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\ie4uinit.exe
```

```
[{89B4C1CD-B018-4511-B0A1-5476DBF70820}] *  
StubPath = C:\WINNT\System32\Rundll32.exe  
C:\WINNT\System32\mscories.dll,Install
```

```
[{9EF0045A-CDD9-438e-95E6-02B9AFEC8E11}] *  
StubPath = %SystemRoot%\System32\updcl.exe -e -u  
%SystemRoot%\System32\verisignpub1.crl
```

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

Registry key not found

Load/Run keys from C:\WINNT\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*

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

HKLM\..\Windows NT\CurrentVersion\Windows: run=*Registry value not found*

HKLM\..\Windows NT\CurrentVersion\Windows: AppInit_DLLs=

Shell & screensaver key from C:\WINNT\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=(NONE)

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:\WINNT\Explorer.exe: PRESENT!

C:\Explorer.exe: not present

C:\WINNT\Explorer\Explorer.exe: not present

C:\WINNT\System\Explorer.exe: not present

C:\WINNT\System32\Explorer.exe: not present

C:\WINNT\Command\Explorer.exe: not present

C:\WINNT\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

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

.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:\WINNT
- .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
6.0\Reader\ActiveX\AcroIEHelper.dll -
{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}

Enumerating Task Scheduler jobs:

No jobs found

Enumerating Download Program Files:

[DirectAnimation Java Classes]

CODEBASE = file://C:\WINNT\Java\classes\dajava.cab

OSD = C:\WINNT\Downloaded Program Files\DirectAnimation Java
Classes.osd

[Microsoft XML Parser for Java]

CODEBASE = file://C:\WINNT\Java\classes\xmldso.cab

OSD = C:\WINNT\Downloaded Program Files\Microsoft XML Parser for
Java.osd

[Office Update Installation Engine]

InProcServer32 = C:\WINNT\opuc.dll

CODEBASE = <http://office.microsoft.com/officeupdate/content/opuc2.cab>

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

[HouseCall Control]

InProcServer32 = C:\WINNT\DOWNLO~1\xscan53.ocx

CODEBASE =

<http://a840.g.akamai.net/7/840/537/2004061001/housecall.trendmicro.com/housecall/xscan53.cab>

[Update Class]

InProcServer32 = C:\WINNT\system32\iuctl.dll

CODEBASE =

<http://v4.windowsupdate.microsoft.com/CAB/x86/unicode/iuctl.CAB?38463.635150463>

[ZoneIntro Class]

InProcServer32 = C:\WINNT\Downloaded Program Files\ZIntro.ocx

CODEBASE = <http://zone.msn.com/binFramework/v10/ZIntro.cab33902.cab>

[Shockwave Flash Object]

InProcServer32 = C:\WINNT\System32\macromed\flash\Flash.ocx

CODEBASE =

<http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>

Enumerating Winsock LSP files:

NameSpace #1: C:\WINNT\System32\rnr20.dll
NameSpace #2: C:\WINNT\System32\winrnr.dll
Protocol #1: C:\WINNT\system32\msafd.dll
Protocol #2: C:\WINNT\system32\msafd.dll
Protocol #3: C:\WINNT\system32\msafd.dll
Protocol #4: C:\WINNT\system32\rsvpsp.dll
Protocol #5: C:\WINNT\system32\rsvpsp.dll
Protocol #6: C:\WINNT\system32\msafd.dll
Protocol #7: C:\WINNT\system32\msafd.dll
Protocol #8: C:\WINNT\system32\msafd.dll
Protocol #9: C:\WINNT\system32\msafd.dll
Protocol #10: C:\WINNT\system32\msafd.dll
Protocol #11: C:\WINNT\system32\msafd.dll
Protocol #12: C:\WINNT\system32\msafd.dll
Protocol #13: C:\WINNT\system32\msafd.dll
Protocol #14: C:\WINNT\system32\msafd.dll
Protocol #15: C:\WINNT\system32\msafd.dll
Protocol #16: C:\WINNT\system32\msafd.dll
Protocol #17: C:\WINNT\system32\msafd.dll

Enumerating Windows NT/2000/XP services

Microsoft ACPI Driver: System32\DRIVERS\ACPI.sys (system)
AFD Networking Support Environment:
\SystemRoot\System32\drivers\afd.sys (autostart)
Alerter: %SystemRoot%\System32\services.exe (manual start)

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

Application Management: %SystemRoot%\system32\services.exe (manual start)
ASP.NET State Service:
%SystemRoot%\Microsoft.NET\Framework\v1.1.4322\aspnet_state.exe (manual start)
RAS Asynchronous Media Driver: System32\DRIVERS\asynmac.sys (manual start)
Standard IDE/ESDI Hard Disk Controller: System32\DRIVERS\atapi.sys (system)
atirage3: System32\DRIVERS\atimpab.sys (manual start)
ATM ARP Client Protocol: System32\DRIVERS\atmarpc.sys (manual start)
Audio Stub Driver: System32\DRIVERS\audstub.sys (manual start)
Background Intelligent Transfer Service:
%SystemRoot%\System32\svchost.exe -k BITSgroup (manual start)
Computer Browser: %SystemRoot%\System32\services.exe (autostart)
Closed Caption Decoder: System32\DRIVERS\CCDECODE.sys (manual start)
SMS Agent Host: C:\WINNT\System32\CCM\CcmExec.exe (autostart)
CD-ROM Driver: System32\DRIVERS\cdrom.sys (system)
Indexing Service: C:\WINNT\System32\cisvc.exe (manual start)
ClipBook: %SystemRoot%\system32\clipsrv.exe (manual start)
Creative SB16/AWE32/AWE64 Driver (WDM): system32\drivers\ctlsb16.sys (manual start)
Cisco Systems VPN Adapter: System32\DRIVERS\CVirtA.sys (manual start)
Cisco Systems, Inc. VPN Service: C:\Program Files\Cisco Systems\VPN Client\cvpnd.exe (autostart)
Cisco Systems Inc. IPsec Driver:
\??\C:\WINNT\System32\Drivers\CVPNDRVA.sys (autostart)
DHCP Client: %SystemRoot%\System32\services.exe (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\services.exe (autostart)
Microsoft DirectMusic SW Synth (WDM): system32\drivers\DMusic.sys (manual start)
Deterministic Network Enhancer Miniport: System32\DRIVERS\dne2000.sys (manual start)
DNS Client: %SystemRoot%\System32\services.exe (autostart)
Print Class Driver for IEEE-1284.4 hpoi07:
System32\DRIVERS\hpoi07.sys (manual start)
Event Log: %SystemRoot%\system32\services.exe (autostart)
COM+ Event System: C:\WINNT\System32\svchost.exe -k netsvcs (manual start)
Fax Service: %systemroot%\system32\faxsvc.exe (manual start)
Floppy Disk Controller Driver: System32\DRIVERS\fdc.sys (manual start)
Floppy Disk Driver: System32\DRIVERS\flpydisk.sys (manual start)
Volume Manager Driver: System32\DRIVERS\ftdisk.sys (system)
Game Port Enumerator: System32\DRIVERS\gameenum.sys (manual start)
Generic Packet Classifier: System32\DRIVERS\msgpc.sys (manual start)

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

IEEE-1284.4 Driver hpoid407: System32\DRIVERS\hpoid407.sys (manual start)
i8042 Keyboard and PS/2 Mouse Port Driver: System32\DRIVERS\i8042prt.sys (system)
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 (manual start)
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\services.exe (autostart)
Workstation: %SystemRoot%\System32\services.exe (autostart)
TCP/IP NetBIOS Helper Service: %SystemRoot%\System32\services.exe (autostart)
Machine Debug Manager: "C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe" (autostart)
Messenger: %SystemRoot%\System32\services.exe (autostart)
NetMeeting Remote Desktop Sharing: C:\WINNT\System32\mnmsrvc.exe (manual start)
Mouse Class Driver: System32\DRIVERS\mouclass.sys (system)
BDA MPE Filter: System32\DRIVERS\MPE.sys (manual start)
MRXSMB: System32\DRIVERS\mrxsmb.sys (system)
Distributed Transaction Coordinator: C:\WINNT\System32\msdtc.exe (manual start)
Microsoft DV Camera and VCR: System32\DRIVERS\msdv.sys (manual start)
Windows Installer: C:\WINNT\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 Streaming Tee/Sink-to-Sink Converter: system32\drivers\MSTEE.sys (manual start)
NABTS/FEC VBI Codec: System32\DRIVERS\NABTSFEC.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)
NeroCd2k: system32\drivers\NeroCd2k.sys (manual start)
NetBIOS Interface: System32\DRIVERS\netbios.sys (system)
NetBios over Tcpip: System32\DRIVERS\netbt.sys (system)
Network DDE: %SystemRoot%\system32\netdde.exe (manual start)
Network DDE DSDM: %SystemRoot%\system32\netdde.exe (manual start)
NetDetect: \SystemRoot\system32\drivers\netdect.sys (manual start)
Net Logon: %SystemRoot%\System32\lsass.exe (autostart)

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

Network Connections: %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
(autostart)
OfficeScanNT RealTime Scan: C:\Program Files\OfficeScan NT\ntrtsan.exe
(autostart)
IPX Traffic Filter Driver: System32\DRIVERS\nwlnkflt.sys (manual start)
IPX Traffic Forwarder Driver: System32\DRIVERS\nwlnkfld.sys (manual
start)
OHCI Compliant IEEE 1394 Host Controller: System32\DRIVERS\ohci1394.sys
(system)
Parallel class driver: System32\DRIVERS\parallel.sys (manual start)
Parallel port driver: System32\DRIVERS\parport.sys (system)
PCI Bus Driver: System32\DRIVERS\pci.sys (system)
PCIIde: System32\DRIVERS\pciide.sys (system)
Plug and Play: %SystemRoot%\system32\services.exe (autostart)
IPSEC Policy Agent: %SystemRoot%\System32\lsass.exe (autostart)
WAN Miniport (PPTP): System32\DRIVERS\raspptp.sys (manual start)
SMS Process Event Driver: \??\C:\WINNT\System32\CCM\prepdv.sys (manual
start)
Protected Storage: %SystemRoot%\system32\services.exe (autostart)
Direct Parallel Link Driver: System32\DRIVERS\ptilink.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)
Direct Parallel: System32\DRIVERS\raspti.sys (manual start)
Microsoft Streaming Network Raw Channel Access:
system32\drivers\RCA.sys (manual start)
Rdbss: System32\DRIVERS\rdbss.sys (system)
Digital CD Audio Playback Filter Driver: System32\DRIVERS\redbook.sys
(system)
Routing and Remote Access: %SystemRoot%\System32\svchost.exe -k netsvcs
(disabled)
Remote Registry Service: %SystemRoot%\system32\regsvc.exe (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 -s (manual start)
Realtek RTL8139/810x/8169/8110 all in one NDIS NT Driver:
system32\DRIVERS\Rtlndis.sys (manual start)
Realtek RTL8139-based PCI Fast Ethernet Adapter NT Driver:
System32\DRIVERS\RTL8139.SYS (manual start)
Remote Administrator Service: "C:\WINNT\system32\explorer.exe" /service

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

(autostart)
Security Accounts Manager: %SystemRoot%\system32\lsass.exe (autostart)
Smart Card Helper: %SystemRoot%\System32\SCardSvr.exe (manual start)
Smart Card: %SystemRoot%\System32\SCardSvr.exe (manual start)
Task Scheduler: %SystemRoot%\system32\MSTask.exe (autostart)
RunAs Service: %SystemRoot%\system32\services.exe (autostart)
System Event Notification: %SystemRoot%\system32\svchost.exe -k netsvcs
(autostart)
Serenum Filter Driver: System32\DRIVERS\serenum.sys (manual start)
Serial port driver: System32\DRIVERS\serial.sys (system)
Internet Connection Sharing: %SystemRoot%\System32\svchost.exe -k
netsvcs (manual start)
BDA Slip De-Framer: System32\DRIVERS\SLIP.sys (manual start)
Sony Memory Stick Driver(SONYPVM1): System32\DRIVERS\SONYPVM1.SYS
(system)
Sony USB Filter Driver (SONYPVU1): System32\DRIVERS\SONYPVU1.SYS
(manual start)
Print Spooler: %SystemRoot%\system32\spoolsv.exe (autostart)
Srv: System32\DRIVERS\srv.sys (manual start)
Still Image Service: %systemroot%\system32\stisvc.exe (autostart)
BDA IPSink: System32\DRIVERS\StreamIP.sys (manual start)
Software Bus Driver: System32\DRIVERS\swenum.sys (manual start)
Microsoft Kernel GS Wavetable Synthesizer: system32\drivers\swmidi.sys
(manual start)
Microsoft 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)
Telnet: %SystemRoot%\system32\tlntsvr.exe (manual start)
Trend Micro Filter: \??\C:\Program Files\OfficeScan NT\TmFilter.sys
(autostart)
OfficeScanNT Listener: C:\Program Files\OfficeScan NT\tmlisten.exe
(autostart)
Distributed Link Tracking Client: %SystemRoot%\system32\services.exe
(autostart)
Microsoft USB Universal Host Controller Driver:
System32\DRIVERS\uhcd.sys (manual start)
Microcode Update Driver: System32\DRIVERS\update.sys (manual start)
Uninterruptible Power Supply: %SystemRoot%\System32\ups.exe (manual
start)
Microsoft USB Standard Hub Driver: System32\DRIVERS\usbhub.sys (manual
start)
USB Mass Storage Driver: System32\DRIVERS\USBSTOR.SYS (manual start)
UsbU2A: System32\Drivers\usbu2a.sys (manual start)
Utility Manager: %SystemRoot%\System32\UtilMan.exe (manual start)
VgaSave: \SystemRoot\System32\drivers\vga.sys (system)
VIA AGP Bus Filter: System32\DRIVERS\viaagp.sys (system)
Trend Micro VSAPI NT: \??\C:\Program Files\OfficeScan NT\VSApiNt.sys
(autostart)

IRC Packets being generated. Dont know where from...

microsoft.public.security.virus: IRC Packets being generated. Dont know where from...

vsdatant: \??\C:\WINNT\System32\vsdatant.sys (manual start)
Windows Time: %SystemRoot%\System32\services.exe (autostart)
Remote Access IP ARP Driver: System32\DRIVERS\wanarp.sys (manual start)
Microsoft WINMM WDM Audio Compatibility Driver:
system32\drivers\wdmaud.sys (manual start)
Windows Management Instrumentation:
%SystemRoot%\System32\WBEM\WinMgmt.exe (autostart)
Windows Management Instrumentation Driver Extensions:
%SystemRoot%\system32\Services.exe (manual start)
World Standard Teletext Codec: System32\DRIVERS\WSTCODEC.SYS (manual start)
Automatic Updates: %systemroot%\system32\svchost.exe -k wugroup (autostart)
Wireless Configuration: %SystemRoot%\System32\svchost.exe -k netsvcs (manual start)

Enumerating Windows NT logon/logoff scripts:

No scripts set to run

Windows NT checkdisk command:

BootExecute = autocheck autochk *

Windows NT 'Wininit.ini':

PendingFileRenameOperations: *Registry value not found*

Enumerating ShellServiceObjectDelayLoad items:

Network.ConnectionTray: C:\WINNT\system32\NETSHELL.dll

WebCheck: C:\WINNT\System32\webcheck.dll

SysTray: stobject.dll

End of report, 27,740 bytes

Report generated in 0.280 seconds

Command line options:

/verbose – to add additional info on each section
/complete – to include empty sections and unsuspecting data
/full – to include several rarely-important sections
/force9x – to include Win9x-only startups even if running on WinNT
/forcent – to include WinNT-only startups even if running on Win9x
/forceall – to include all Win9x and WinNT startups, regardless of platform
/history – to list version history only

IRC Packets being generated. Dont know where from...