Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1, Task ID: 2

Task ID:	2
Risk Level:	10
Date Processed:	2016-03-28 07:35:09 (UTC)
Processing Time:	62.36 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\spyeye_injector.exe"

Sample ID:	1
Type:	basic
Owner:	admin
Label:	spyeye_injector.exe
Date Added:	2016-03-28 07:35:09 (UTC)
File Type:	PE32:win32:gui
File Size:	103936 bytes
MD5:	b98bb6d7428c3dbffcfcab2414c6daa2
SHA256:	fc7f54ce456c164452d8429a7fd5f52629a69338f8954e287d2664c03c37e029
Description:	None

Pattern Matching Results

7	Writes to memory of system processes
6	Modifies registry autorun entries
3	HTTP connection - response code 200 (success)
10	Suspicious writeprocess: Spyeye [Banking]
5	Abnormal sleep detected
5	Installs service
8	Possible kernel API resolver
6	Writes to system32 folder
2	PE: Nonstandard section
3	Writes to a log file [Info]
3	Long sleep detected
4	Reads process memory
5	PE: Contains compressed section
5	Packer: UPX
5	Adds autostart object
10	Creates malicious mutex: Spyeye [Banking]

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\spyeye_injector.exe ["c:\windows\temp\spyeye_injector.exe"]
Creates process:	C:\WinOldFileq\83A49421643.exe ["C:\WinOldFileq\83A49421643.exe"]
Reads from process:	PID:1192 C:\WINDOWS\system32\calc.exe
Reads from process:	PID:1272 C:\WINDOWS\system32\svchost.exe
Reads from process:	PID:1896 C:\WINDOWS\explorer.exe
Writes to process:	PID:1896 C:\WINDOWS\explorer.exe
Writes to process:	PID:592 C:\WINDOWS\system32\winlogon.exe
Writes to process:	PID:908 C:\WINDOWS\system32\lsass.exe
Writes to process:	PID:1068 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1148 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1272 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1340 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID:1732 C:\WINDOWS\system32\spoolsv.exe
Writes to process:	PID:1956 C:\Program Files\Java\jre7\bin\jqs.exe
Writes to process:	PID:272 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Writes to process:	PID:292 C:\WINDOWS\system32\ctfmon.exe
Writes to process:	PID:1208 C:\WINDOWS\system32\alg.exe
Writes to process:	PID:1416 C:\WINDOWS\system32\rundll32.exe
Writes to process:	PID:520 C:\WINDOWS\system32\wbem\unsecapp.exe
Writes to process:	PID:180 C:\WINDOWS\system32\wbem\wmiprvse.exe
Writes to process:	PID:1616 C:\WINDOWS\Temp\spyeye_injector.exe
Terminates process:	C:\WinOldFileq\83A49421643.exe
Terminates process:	C:\WINDOWS\Temp\spyeye_injector.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\RPCController
Creates mutex:	\BaseNamedObjects\zXeRY3a_PtW|00000000
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local settings!temporary internet files!content.ie5!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!cookies!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!

```
  Creates mutex:          \BaseNamedObjects\WininetConnectionMutex
  Creates mutex:          \BaseNamedObjects\WCcUCYUwUES99KYIA9O7qMES7KQ1e
  Creates mutex:          \BaseNamedObjects\MSPMutex
  Creates mutex:          \BaseNamedObjects\RAS_MO_02
  Creates mutex:          \BaseNamedObjects\RAS_MO_01
  Creates mutex:          \BaseNamedObjects\MSCTF.Shared.MUTEX.MGH
  Creates event:          \BaseNamedObjects\crypt32LogoffEvent
  Creates event:
\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000007B8.00000000.00000004
  Creates event:          \BaseNamedObjects\CTF.ThreadMIConnectionEvent.000007B8.00000000.00000004
  Creates event:          \BaseNamedObjects\MSCTF.SendReceive.Event.ILH.IC
  Creates event:          \BaseNamedObjects\MSCTF.SendReceiveConection.Event.ILH.IC
  Creates event:          \BaseNamedObjects\MSCTF.SendReceive.Event.MGH.IC
  Creates event:          \BaseNamedObjects\MSCTF.SendReceiveConection.Event.MGH.IC
  Creates semaphore:      \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
  Creates semaphore:      \BaseNamedObjects\4FBEA4B1
```

File System Events

```
  Creates:                C:\WinOldFileq
  Creates:                C:\WinOldFileq\
  Creates:                C:\WinOldFileq\83A49421643.exe
  Creates:                C:\WinOldFileq\B20776D7F8FB639
  Creates:                C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
  Creates:                C:\Documents and Settings\Admin\Cookies\admin@microsoft[2].txt
  Creates:                C:\WINDOWS\Prefetch\NTOSBOOT-B00DFAAD.pf
  Creates:                C:\WINDOWS\Prefetch\RUNDLL32.EXE-18273726.pf
  Creates:                C:\WINDOWS\Prefetch\PYTHONW.EXE-1A630664.pf
  Creates:                C:\WINDOWS\Prefetch\REG.EXE-0D2A95F7.pf
  Creates:                C:\WINDOWS\Prefetch\SC.EXE-012262AF.pf
  Creates:                C:\WINDOWS\Prefetch\IVM-SERVICE.EXE-074ABCAF.pf
  Creates:                C:\WINDOWS\Prefetch\83A49421643.EXE-1FEF9BA6.pf
  Creates:                C:\WINDOWS\Prefetch\UNSECAPP.EXE-1A95A33B.pf
  Creates:                C:\WINDOWS\Prefetch\SPYEYE_INJECTOR.EXE-255B270C.pf
  Creates:                C:\WINDOWS\Prefetch\WMIPRVSE.EXE-28F301A9.pf
  Creates:                C:\WINDOWS\Prefetch\PARANORMAL.EXE-05B653A9.pf
  Creates:                C:\WINDOWS\Prefetch\CALC.EXE-02CD573A.pf
  Opens:                  C:\WINDOWS\Prefetch\SPYEYE_INJECTOR.EXE-255B270C.pf
  Opens:                  C:\Documents and Settings\Admin
  Opens:                  C:\WINDOWS\system32\kernel32.dll
  Opens:                  C:\
  Opens:                  C:\WINDOWS\system32\ntdll.dll
  Opens:                  C:\WinOldFileq
  Opens:                  C:\WinOldFileq\
  Opens:                  C:\WINDOWS\Temp\spyeye_injector.exe
  Opens:                  C:\WINDOWS\system32\drprov.dll
  Opens:                  C:\WINDOWS\system32\ntlanman.dll
  Opens:                  C:\WINDOWS\system32\netui0.dll
  Opens:                  C:\WINDOWS\system32\netui1.dll
  Opens:                  C:\WINDOWS\system32\netrap.dll
  Opens:                  C:\WINDOWS\system32\samlib.dll
  Opens:                  C:\WINDOWS\system32\davclnt.dll
  Opens:                  C:\WinOldFileq\83A49421643.exe
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WinOldFileq\83A49421643.exe.Manifest
  Opens:                  C:\WINDOWS\Temp\3478ca70-4a52-4ef0-b743-9c90c5d6fcfc
  Opens:                  C:\WINDOWS\Prefetch\83A49421643.EXE-1FEF9BA6.pf
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\imm32.dll
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                  C:\WINDOWS\WindowsShell.Manifest
  Opens:                  C:\WINDOWS\WindowsShell.Config
  Opens:                  C:\WINDOWS\system32\WININET.dll.123.Manifest
  Opens:                  C:\WINDOWS\system32\WININET.dll.123.Config
  Opens:                  C:\WINDOWS\system32\msimg32.dll
  Opens:                  C:\WINDOWS\system32\shell32.dll
  Opens:                  C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:                  C:\WINDOWS\system32\comctl32.dll
  Opens:                  C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\comctl32.dll.124.Config
  Opens:                  C:\WinOldFileq\B20776D7F8FB639
  Opens:                  C:\WINDOWS\system32\user32.dll
  Opens:                  C:\WINDOWS\system32\wininet.dll
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
  Opens:                 C:\Documents and Settings\Admin\Local Settings\History
  Opens:                 C:\WINDOWS\system32\advapi32.dll
  Opens:                 C:\Documents and Settings\Admin\Local Settings\History\History.IE5
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
  Opens:                 C:\Documents and Settings\Admin\Cookies
  Opens:                 C:\Documents and Settings\Admin\Cookies\index.dat
  Opens:                 C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
  Opens:                 C:\WINDOWS\system32\mswsock.dll
  Opens:                 C:\WINDOWS\system32\hnetcfg.dll
  Opens:                 C:\WINDOWS\system32\wshtcpip.dll
  Opens:                 C:\AUTOEXEC.BAT
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CTLs
  Opens:                 C:\windows\temp\spyeye_injector.exe
  Opens:                 C:\WINDOWS\system32\MSCTF.dll
  Opens:                 C:\WINDOWS\system32\wbem\Repository\$WinMgmt.CFG
  Opens:                 C:\WINDOWS\system32\rasapi32.dll
  Opens:                 C:\WINDOWS\system32\rasman.dll
  Opens:                 C:\WINDOWS\system32\tapi32.dll
  Opens:                 C:\WINDOWS\system32\TAPI32.dll.124.Manifest
  Opens:                 C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:                 C:\WINDOWS\system32\tapisrv.dll
  Opens:                 C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
  Opens:                 C:\WINDOWS\system32\ras
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
  Opens:                 C:\WINDOWS\system32\rasmans.dll
  Opens:                 C:\WINDOWS\system32\sensapi.dll
  Opens:                 C:\WINDOWS\system32\winipsec.dll
  Opens:                 C:\WINDOWS\system32\rasadhlp.dll
  Opens:                 C:\WINDOWS\system32\rastapi.dll
  Opens:                 C:\WINDOWS\system32\dnsapi.dll
  Opens:                 C:\WINDOWS\system32\sens.dll
  Opens:                 C:\WINDOWS\system32\wbem\Logs\wbemess.log
  Opens:                 C:\WINDOWS\system32\winrnr.dll
  Opens:                 C:\WINDOWS\system32\mprapi.dll
  Opens:                 C:\WINDOWS\system32\activeds.dll
  Opens:                 C:\WINDOWS\system32\adsldpc.dll
  Opens:                 C:\WINDOWS\system32\unimdm.tsp
  Opens:                 C:\WINDOWS\system32\uniplat.dll
  Opens:                 C:\WINDOWS\system32\kmddsp.tsp
  Opens:                 C:\WINDOWS\system32\ndptsp.tsp
  Opens:                 C:\WINDOWS\system32\ipconf.tsp
  Opens:                 C:\WINDOWS\system32\calc.exe
  Opens:                 C:\WINDOWS\system32\h323.tsp
  Opens:                 C:\WINDOWS\system32\h323log.txt
  Opens:                 C:\WINDOWS\system32\hidphone.tsp
  Opens:                 C:\WINDOWS\system32\hid.dll
  Opens:                 C:\WINDOWS\system32\rasppp.dll
  Opens:                 C:\WINDOWS\system32\ntlsapi.dll
  Opens:                 C:\WINDOWS\system32\kerberos.dll
  Opens:                 C:\WINDOWS\system32\cryptdll.dll
  Opens:                 C:\WINDOWS\win.ini
  Opens:                 C:\WINDOWS\system32\rasqec.dll
  Opens:                 C:\WINDOWS\system32\msv1_0.dll
  Opens:                 C:\WINDOWS\system32\MSIMTF.dll
  Opens:                 C:\Program Files\Java\jre7\bin\client
  Opens:                 C:\Program Files\Java\jre7\bin\client\classes.jsa
  Opens:                 C:\WINDOWS\system32\setupapi.dll
  Opens:                 C:\Program Files\Java\jre7\lib
  Opens:                 C:\Program Files\Java\jre7\lib\content-types.properties
  Opens:                 C:\Program Files\Java\jre7\lib\deploy.jar
  Opens:                 C:\Program Files\Java\jre7\lib\ext
  Opens:                 C:\Program Files\Java\jre7\lib\ext\dnsns.jar
  Opens:                 C:\Program Files\Java\jre7\lib\ext\localedata.jar
  Opens:                 C:\Program Files\Java\jre7\lib\fontconfig.bfc
  Opens:                 C:\Program Files\Java\jre7\lib\fonts
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaBrightDemiBold.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaBrightDemiItalic.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaBrightItalic.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaBrightRegular.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaSansDemiBold.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaSansRegular.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaTypewriterBold.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\fonts\LucidaTypewriterRegular.ttf
  Opens:                 C:\Program Files\Java\jre7\lib\javaws.jar
  Opens:                 C:\Program Files\Java\jre7\lib\jsse.jar
  Opens:                 C:\Program Files\Java\jre7\lib\logging.properties
  Opens:                 C:\Program Files\Java\jre7\lib\meta-index
  Opens:                 C:\Program Files\Java\jre7\lib\net.properties
  Opens:                 C:\Program Files\Java\jre7\lib\plugin.jar
  Opens:                 C:\Program Files\Java\jre7\lib\resources.jar
  Opens:                 C:\Program Files\Java\jre7\lib\rt.jar
  Opens:                 C:\Program Files\Java\jre7\lib\security
  Opens:                 C:\Program Files\Java\jre7\lib\security\blacklist
  Opens:                 C:\Program Files\Java\jre7\lib\security\java.policy
  Opens:                 C:\Program Files\Java\jre7\lib\security\java.security
  Opens:                 C:\Program Files\Java\jre7\lib\security\javaws.policy
  Opens:                 C:\Program Files\Java\jre7\lib\tzmappings
  Opens:                 C:\Program Files\Java\jre7\lib\zi
  Opens:                 C:\Program Files\Java\jre7\lib\zi\GMT
  Opens:                 C:\Program Files\Java\jre7\bin
  Opens:                 C:\Program Files\Java\jre7\bin\awt.dll
  Opens:                 C:\Program Files\Java\jre7\bin\client\jvm.dll
  Opens:                 C:\Program Files\Java\jre7\bin\dcpr.dll
  Opens:                 C:\Program Files\Java\jre7\bin\deploy.dll
  Opens:                 C:\Program Files\Java\jre7\bin\fontmanager.dll
  Opens:                 C:\Program Files\Java\jre7\bin\java.dll
  Opens:                 C:\Program Files\Java\jre7\bin\javaw.exe
  Opens:                 C:\Program Files\Java\jre7\bin\jp2native.dll
  Opens:                 C:\Program Files\Java\jre7\bin\jpeg.dll
  Opens:                 C:\Program Files\Java\jre7\bin\msvcr100.dll
  Opens:                 C:\Program Files\Java\jre7\bin\net.dll
  Opens:                 C:\Program Files\Java\jre7\bin\nio.dll
  Opens:                 C:\Program Files\Java\jre7\bin\verify.dll
  Opens:                 C:\Program Files\Java\jre7\bin\zip.dll
  Opens:                 C:\WINDOWS\system32\drivers\etc\hosts
  Opens:                 C:\WINDOWS\system32\rsaenh.dll
  Opens:                 C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
  Opens:                 C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
  Opens:                 C:\WINDOWS\Prefetch\NTOSBOOT-BOODFAAD.pf
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\Protect\CREDHIST
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\3ea8a527-1704-4983-8596-ab49c663cca3
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\4f5d6884-c60c-4cd3-906b-3d677949fac1
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003\fe1a937a-0ac9-4cf1-978d-5d0742ed2858
  Opens:                 C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons\SP_6A65DB879F95470886BD7EFE4977B10E.dat
  Opens:                 C:\Documents and Settings\Admin\Favorites\Desktop.ini
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\IconCache.db
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache\index.dat
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer\MSIMGSIZ.DAT
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
  Opens:                 C:\Documents and Settings\Admin\Local Settings\desktop.ini
  Opens:                 C:\Documents and Settings\Admin\Local Settings\History\desktop.ini
  Opens:                 C:\DOCUMENTS AND SETTINGS\ADMIN\LOCAL
SETTINGS\HISTORY\HISTORY.IE5\MSHIST012014040420140405\INDEX.DAT
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR\favicon[1].ico
  Opens:                 C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:                 C:\Documents and Settings\Admin\NTUSER.DAT
  Opens:                 C:\Documents and Settings\Admin\ntuser.ini
  Opens:                 C:\Documents and Settings\Admin\Start Menu\desktop.ini
  Opens:                 C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Opens:                 C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Magnifier.lnk
  Opens:                 C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Narrator.lnk
  Opens:                 C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\On-Screen Keyboard.lnk
  Opens:                 C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility\Utility Manager.lnk
  Opens:                 C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Address
Book.lnk
  Opens:                 C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Command
Prompt.lnk
  Opens:                 C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\desktop.ini
```

```
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment\Windows Media Player.lnk
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Notepad.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Program
Compatibility Wizard.lnk
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Synchronize.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools\Internet Explorer (No Add-ons).lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Tour
Windows XP.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\Windows
Explorer.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\desktop.ini
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Internet
Explorer.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Outlook Express.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Remote
Assistance.lnk
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Startup\desktop.ini
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Windows Media
Player.lnk
  Opens:                  C:\Documents and Settings\All Users\Application Data\Microsoft\User
Account Pictures\Admin.bmp
  Opens:                  C:\Documents and Settings\All Users\Desktop\Adobe Reader 9.lnk
  Opens:                  C:\Documents and Settings\All Users\Documents\desktop.ini
  Opens:                  C:\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\ACTIVATE WINDOWS.LNK
  Opens:                  C:\Documents and Settings\All Users\Start Menu\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility\Accessibility Wizard.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Calculator.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\HyperTerminal.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Network Connections.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Network Setup Wizard.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\New Connection Wizard.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications\Wireless Network Setup Wizard.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Sound Recorder.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment\Volume Control.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Paint.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Remote Desktop Connection.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Activate Windows.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Backup.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Character Map.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\desktop.ini
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Cleanup.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Disk Defragmenter.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Files and Settings Transfer Wizard.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Scheduled Tasks.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\Security Center.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Information.lnk
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools\System Restore.lnk
```

```
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\WordPad.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Component Services.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Computer Management.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Data Sources (ODBC).lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\desktop.ini
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Event Viewer.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Local Security Policy.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Performance.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools\Services.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Adobe Reader
9.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\desktop.ini
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Games\desktop.ini
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Freecell.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Hearts.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Backgammon.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Checkers.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Hearts.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Reversi.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Internet
Spades.lnk
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Minesweeper.lnk
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Pinball.lnk
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Games\Solitaire.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Games\Spider
Solitaire.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
Excel Viewer.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office
Word Viewer 2003.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Microsoft
PowerPoint Viewer .lnk
  Opens:                 C:\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\PROGRAMS\MICROSOFT
SILVERLIGHT\MICROSOFT SILVERLIGHT.LNK
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\MSN.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7\IDLE
(Python GUI).lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Module Docs.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python (command line).lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python for Windows Documentation.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Python Manuals.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\PythonWin.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Python
2.7\Uninstall Python.lnk
  Opens:                 C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\desktop.ini
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Windows
Messenger.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Programs\Windows Movie
Maker.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Set Program Access and
Defaults.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Windows Catalog.lnk
  Opens:                 C:\Documents and Settings\All Users\Start Menu\Windows Update.lnk
  Opens:                 C:\Documents and Settings\LocalService\Cookies\index.dat
  Opens:                 C:\Documents and Settings\LocalService\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
  Opens:                 C:\Documents and Settings\LocalService\Local Settings\desktop.ini
  Opens:                 C:\Documents and Settings\LocalService\Local
Settings\History\History.IE5\index.dat
```

```
  Opens:                 C:\Documents and Settings\LocalService\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
  Opens:                 C:\Documents and Settings\LocalService\NTUSER.DAT
  Opens:                 C:\Documents and Settings\NetworkService\Local Settings\Application
Data\Microsoft\Windows\UsrClass.dat
  Opens:                 C:\Documents and Settings\NetworkService\Local Settings\desktop.ini
  Opens:                 C:\Documents and Settings\NetworkService\NTUSER.DAT
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temp\AdobeARM.log
  Opens:                 C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
  Opens:                 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
  Opens:                 C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
  Opens:                 C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
  Opens:                 C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe
  Opens:                 C:\Program Files\Common Files\Java\Java Update\jusched.exe
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\MSInfo\msinfo32.exe
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\Speech\sapi.dll
  Opens:                 C:\Program Files\Common
Files\SpeechEngines\Microsoft\Lexicon\1033\ltts1033.lxa
  Opens:                 C:\Program Files\Common
Files\SpeechEngines\Microsoft\Lexicon\1033\r1033tts.lxa
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\spcommon.dll
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS\1033\sam.sdf
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS\1033\sam.spd
  Opens:                 C:\Program Files\Common
Files\SpeechEngines\Microsoft\TTS\1033\spttseng.dll
  Opens:                 C:\Program Files\Internet Explorer\ieproxy.dll
  Opens:                 C:\Program Files\Internet Explorer\iexplore.exe
  Opens:                 C:\Program Files\Internet Explorer\sqmapi.dll
  Opens:                 C:\Program Files\Internet Explorer\xpshims.dll
  Opens:                 C:\Program Files\Java\jre7\bin\jp2ssv.dll
  Opens:                 C:\Program Files\Java\jre7\bin\jqs.exe
  Opens:                 C:\Program Files\Java\jre7\lib\deploy\jqs\jqs.conf
  Opens:                 C:\Program Files\Messenger\msmsgs.exe
  Opens:                 C:\Program Files\Movie Maker\moviemk.exe
  Opens:                 C:\Program Files\MSN Gaming Zone\Windows\bckgzm.exe
  Opens:                 C:\Program Files\MSN Gaming Zone\Windows\chkrzm.exe
  Opens:                 C:\Program Files\MSN Gaming Zone\Windows\hrtzzm.exe
  Opens:                 C:\Program Files\MSN Gaming Zone\Windows\Rvsezm.exe
  Opens:                 C:\Program Files\MSN Gaming Zone\Windows\shvlzm.exe
  Opens:                 C:\Program Files\MSN\MSNCoreFiles\Install\msnms.ico
  Opens:                 C:\Program Files\Outlook Express\msimn.exe
  Opens:                 C:\Program Files\Outlook Express\wab.exe
  Opens:                 C:\Program Files\Windows Media Player\wmplayer.exe
  Opens:                 C:\Program Files\Windows NT\Accessories\wordpad.exe
  Opens:                 C:\Program Files\Windows NT\hypertrm.exe
  Opens:                 C:\Program Files\Windows NT\Pinball\PINBALL.EXE
  Opens:                 C:\System Volume Information\tracking.log
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\drivetable.txt
  Opens:                 C:\SYSTEM VOLUME INFORMATION\_RESTORE{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP22\CHANGE.LOG
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP22\rp.log
  Opens:                 C:\SYSTEM VOLUME INFORMATION\_RESTORE{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP24\CHANGE.LOG
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP24\rp.log
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP25\change.log
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP25\rp.log
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\_driver.cfg
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\_filelst.cfg
  Opens:                 C:\WINDOWS\AppPatch\AcAdProc.dll
  Opens:                 C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:                 C:\WINDOWS\AppPatch\drvmain.sdb
  Opens:                 C:\WINDOWS\bootstat.dat
  Opens:                 C:\WINDOWS\Debug\UserMode\userenv.log
  Opens:                 C:\WINDOWS\explorer.exe
  Opens:                 C:\WINDOWS\Fonts\arial.ttf
  Opens:                 C:\WINDOWS\Fonts\arialbd.ttf
  Opens:                 C:\WINDOWS\Fonts\arialbi.ttf
  Opens:                 C:\WINDOWS\Fonts\ariali.ttf
  Opens:                 C:\WINDOWS\Fonts\ariblk.ttf
  Opens:                 C:\WINDOWS\Fonts\CALIBRI.TTF
  Opens:                 C:\WINDOWS\Fonts\CALIBRIB.TTF
  Opens:                 C:\WINDOWS\Fonts\CALIBRII.TTF
  Opens:                 C:\WINDOWS\Fonts\CALIBRIZ.TTF
  Opens:                 C:\WINDOWS\Fonts\CAMBRIA.TTC
  Opens:                 C:\WINDOWS\Fonts\CAMBRIAB.TTF
  Opens:                 C:\WINDOWS\Fonts\CAMBRIAI.TTF
```

```
Opens:                        C:\WINDOWS\Fonts\CAMBRIAZ.TTF
Opens:                        C:\WINDOWS\Fonts\CANDARA.TTF
Opens:                        C:\WINDOWS\Fonts\CANDARAB.TTF
Opens:                        C:\WINDOWS\Fonts\CANDARAI.TTF
Opens:                        C:\WINDOWS\Fonts\CANDARAZ.TTF
Opens:                        C:\WINDOWS\Fonts\cga40woa.fon
Opens:                        C:\WINDOWS\Fonts\cga80woa.fon
Opens:                        C:\WINDOWS\Fonts\comic.ttf
Opens:                        C:\WINDOWS\Fonts\comicbd.ttf
Opens:                        C:\WINDOWS\Fonts\CONSOLA.TTF
Opens:                        C:\WINDOWS\Fonts\CONSOLAB.TTF
Opens:                        C:\WINDOWS\Fonts\CONSOLAI.TTF
Opens:                        C:\WINDOWS\Fonts\CONSOLAZ.TTF
Opens:                        C:\WINDOWS\Fonts\CONSTAN.TTF
Opens:                        C:\WINDOWS\Fonts\CONSTANB.TTF
Opens:                        C:\WINDOWS\Fonts\CONSTANI.TTF
Opens:                        C:\WINDOWS\Fonts\CONSTANZ.TTF
Opens:                        C:\WINDOWS\Fonts\CORBEL.TTF
Opens:                        C:\WINDOWS\Fonts\CORBELB.TTF
Opens:                        C:\WINDOWS\Fonts\CORBELI.TTF
Opens:                        C:\WINDOWS\Fonts\CORBELZ.TTF
Opens:                        C:\WINDOWS\Fonts\cour.ttf
Opens:                        C:\WINDOWS\Fonts\courbd.ttf
Opens:                        C:\WINDOWS\Fonts\courbi.ttf
Opens:                        C:\WINDOWS\Fonts\coure.fon
Opens:                        C:\WINDOWS\Fonts\couri.ttf
Opens:                        C:\WINDOWS\Fonts\dosapp.fon
Opens:                        C:\WINDOWS\Fonts\ega40woa.fon
Opens:                        C:\WINDOWS\Fonts\ega80woa.fon
Opens:                        C:\WINDOWS\Fonts\estre.ttf
Opens:                        C:\WINDOWS\Fonts\framd.ttf
Opens:                        C:\WINDOWS\Fonts\framdit.ttf
Opens:                        C:\WINDOWS\Fonts\gautami.ttf
Opens:                        C:\WINDOWS\Fonts\georgia.ttf
Opens:                        C:\WINDOWS\Fonts\georgiab.ttf
Opens:                        C:\WINDOWS\Fonts\georgiai.ttf
Opens:                        C:\WINDOWS\Fonts\georgiaz.ttf
Opens:                        C:\WINDOWS\Fonts\GlobalMonospace.CompositeFont
Opens:                        C:\WINDOWS\Fonts\GlobalSansSerif.CompositeFont
Opens:                        C:\WINDOWS\Fonts\GlobalSerif.CompositeFont
Opens:                        C:\WINDOWS\Fonts\GlobalUserInterface.CompositeFont
Opens:                        C:\WINDOWS\Fonts\impact.ttf
Opens:                        C:\WINDOWS\Fonts\latha.ttf
Opens:                        C:\WINDOWS\Fonts\lucon.ttf
Opens:                        C:\WINDOWS\Fonts\l_10646.ttf
Opens:                        C:\WINDOWS\Fonts\mangal.ttf
Opens:                        C:\WINDOWS\Fonts\marlett.ttf
Opens:                        C:\WINDOWS\Fonts\MEIRYO.TTC
Opens:                        C:\WINDOWS\Fonts\MEIRYOB.TTC
Opens:                        C:\WINDOWS\Fonts\micross.ttf
Opens:                        C:\WINDOWS\Fonts\modern.fon
Opens:                        C:\WINDOWS\Fonts\mvboli.ttf
Opens:                        C:\WINDOWS\Fonts\pala.ttf
Opens:                        C:\WINDOWS\Fonts\palab.ttf
Opens:                        C:\WINDOWS\Fonts\palabi.ttf
Opens:                        C:\WINDOWS\Fonts\palai.ttf
Opens:                        C:\WINDOWS\Fonts\raavi.ttf
Opens:                        C:\WINDOWS\Fonts\roman.fon
Opens:                        C:\WINDOWS\Fonts\script.fon
Opens:                        C:\WINDOWS\Fonts\SEGOEUI.TTF
Opens:                        C:\WINDOWS\Fonts\SEGOEUIB.TTF
Opens:                        C:\WINDOWS\Fonts\SEGOEUII.TTF
Opens:                        C:\WINDOWS\Fonts\SEGOEUIZ.TTF
Opens:                        C:\WINDOWS\Fonts\serife.fon
Opens:                        C:\WINDOWS\Fonts\shruti.ttf
Opens:                        C:\WINDOWS\Fonts\smalle.fon
Opens:                        C:\WINDOWS\Fonts\sserife.fon
Opens:                        C:\WINDOWS\Fonts\sylfaen.ttf
Opens:                        C:\WINDOWS\Fonts\symbol.ttf
Opens:                        C:\WINDOWS\Fonts\symbole.fon
Opens:                        C:\WINDOWS\Fonts\tahoma.ttf
Opens:                        C:\WINDOWS\Fonts\tahomabd.ttf
Opens:                        C:\WINDOWS\Fonts\times.ttf
Opens:                        C:\WINDOWS\Fonts\timesbd.ttf
Opens:                        C:\WINDOWS\Fonts\timesbi.ttf
Opens:                        C:\WINDOWS\Fonts\timesi.ttf
Opens:                        C:\WINDOWS\Fonts\trebuc.ttf
Opens:                        C:\WINDOWS\Fonts\trebucbd.ttf
Opens:                        C:\WINDOWS\Fonts\trebucbi.ttf
Opens:                        C:\WINDOWS\Fonts\trebucit.ttf
Opens:                        C:\WINDOWS\Fonts\tunga.ttf
Opens:                        C:\WINDOWS\Fonts\verdana.ttf
Opens:                        C:\WINDOWS\Fonts\verdanab.ttf
```

```
  Opens:                 C:\WINDOWS\Fonts\verdanai.ttf
  Opens:                 C:\WINDOWS\Fonts\verdanaz.ttf
  Opens:                 C:\WINDOWS\Fonts\vgafix.fon
  Opens:                 C:\WINDOWS\Fonts\vgaoem.fon
  Opens:                 C:\WINDOWS\Fonts\vgasys.fon
  Opens:                 C:\WINDOWS\Fonts\webdings.ttf
  Opens:                 C:\WINDOWS\Fonts\wingding.ttf
  Opens:                 C:\WINDOWS\Fonts\wst_czec.fon
  Opens:                 C:\WINDOWS\Fonts\wst_engl.fon
  Opens:                 C:\WINDOWS\Fonts\wst_fren.fon
  Opens:                 C:\WINDOWS\Fonts\wst_germ.fon
  Opens:                 C:\WINDOWS\Fonts\wst_ital.fon
  Opens:                 C:\WINDOWS\Fonts\wst_span.fon
  Opens:                 C:\WINDOWS\Fonts\wst_swed.fon
  Opens:                 C:\WINDOWS\hh.exe
  Opens:                 C:\WINDOWS\ime\SPTIP.dll
  Opens:                 C:\WINDOWS\INSTALLER\{89F4137D-6C26-4A84-BDB8-
2E5A4BB71E00}\CONFIGICONDLL
  Opens:                 C:\WINDOWS\Installer\{90850409-6000-11D3-8CFE-0150048383C9}\wrdvicon.exe
  Opens:                 C:\WINDOWS\Installer\{95120000-003F-0409-0000-0000000FF1CE}\xlvwicon.exe
  Opens:                 C:\WINDOWS\Installer\{95140000-00AF-0409-0000-0000000FF1CE}\ppvwicon.exe
  Opens:                 C:\WINDOWS\Installer\{AC76BA86-7AD7-1033-7B44-
A93000000001}\SC_Reader.ico
  Opens:                 C:\WINDOWS\Installer\{C3CC4DF5-39A5-4027-B136-
2B3E1F5AB6E2}\python_icon.exe
  Opens:                 C:\WINDOWS\pchealth\helpctr\binaries\pchsvc.dll
  Opens:                 C:\Documents and Settings\Admin\Cookies\admin@microsoft[2].txt
  Opens:                 C:\WINDOWS\Registration\R000000000007.clb
  Opens:                 C:\WINDOWS\Resources\Themes\Luna\luna.msstyles
  Opens:                 C:\WINDOWS\SchedLgU.Txt
  Opens:                 C:\WINDOWS\setuplog.txt
  Opens:                 C:\WINDOWS\system.ini
  Opens:                 C:\WINDOWS\system32\$winnt$.inf
  Opens:                 C:\WINDOWS\system32\accwiz.exe
  Opens:                 C:\WINDOWS\system32\actxprxy.dll
  Opens:                 C:\WINDOWS\system32\alg.exe
  Opens:                 C:\WINDOWS\system32\apphelp.dll
  Opens:                 C:\WINDOWS\system32\atl.dll
  Opens:                 C:\WINDOWS\system32\atmfd.dll
  Opens:                 C:\WINDOWS\system32\audiosrv.dll
  Opens:                 C:\WINDOWS\system32\authz.dll
  Opens:                 C:\WINDOWS\system32\autochk.exe
  Opens:                 C:\WINDOWS\system32\basesrv.dll
  Opens:                 C:\WINDOWS\system32\batmeter.dll
  Opens:                 C:\WINDOWS\system32\browser.dll
  Opens:                 C:\WINDOWS\system32\browseui.dll
  Opens:                 C:\WINDOWS\system32\certcli.dll
  Opens:                 C:\WINDOWS\system32\charmap.exe
  Opens:                 C:\WINDOWS\system32\clbcatq.dll
  Opens:                 C:\WINDOWS\system32\cleanmgr.exe
  Opens:                 C:\WINDOWS\system32\clusapi.dll
  Opens:                 C:\WINDOWS\system32\cmd.exe
  Opens:                 C:\WINDOWS\system32\cnbjmon.dll
  Opens:                 C:\WINDOWS\system32\colbact.dll
  Opens:                 C:\WINDOWS\system32\comdlg32.dll
  Opens:                 C:\WINDOWS\system32\compatUI.dll
  Opens:                 C:\WINDOWS\system32\comres.dll
  Opens:                 C:\WINDOWS\system32\comsvcs.dll
  Opens:                 C:\WINDOWS\system32\config\AppEvent.Evt
  Opens:                 C:\WINDOWS\system32\config\Internet.evt
  Opens:                 C:\WINDOWS\system32\config\SecEvent.Evt
  Opens:                 C:\WINDOWS\system32\config\SysEvent.Evt
  Opens:                 C:\WINDOWS\system32\credui.dll
  Opens:                 C:\WINDOWS\system32\cryptnet.dll
  Opens:                 C:\WINDOWS\system32\cryptsvc.dll
  Opens:                 C:\WINDOWS\system32\cryptui.dll
  Opens:                 C:\WINDOWS\system32\cscdll.dll
  Opens:                 C:\WINDOWS\system32\cscui.dll
  Opens:                 C:\WINDOWS\system32\csrsrv.dll
  Opens:                 C:\WINDOWS\system32\csrss.exe
  Opens:                 C:\WINDOWS\system32\ctfmon.exe
  Opens:                 C:\WINDOWS\system32\ctype.nls
  Opens:                 C:\WINDOWS\system32\c_1250.nls
  Opens:                 C:\WINDOWS\system32\c_1251.nls
  Opens:                 C:\WINDOWS\system32\c_1253.nls
  Opens:                 C:\WINDOWS\system32\desk.cpl
  Opens:                 C:\WINDOWS\system32\dfrgres.dll
  Opens:                 C:\WINDOWS\system32\dhcpcsvc.dll
  Opens:                 C:\WINDOWS\system32\dimsntfy.dll
  Opens:                 C:\WINDOWS\system32\dmserver.dll
  Opens:                 C:\WINDOWS\system32\dnsrslvr.dll
  Opens:                 C:\WINDOWS\system32\dot3api.dll
  Opens:                 C:\WINDOWS\system32\dot3dlg.dll
```

```
Opens:                  C:\WINDOWS\system32\dpcdll.dll
Opens:                  C:\WINDOWS\system32\drivers\afd.sys
Opens:                  C:\WINDOWS\system32\drivers\audstub.sys
Opens:                  C:\WINDOWS\system32\drivers\beep.sys
Opens:                  C:\WINDOWS\system32\drivers\cdaudio.sys
Opens:                  C:\WINDOWS\system32\drivers\cdfs.sys
Opens:                  C:\WINDOWS\system32\drivers\cdrom.sys
Opens:                  C:\WINDOWS\system32\drivers\CmBatt.sys
Opens:                  C:\WINDOWS\system32\drivers\dxapi.sys
Opens:                  C:\WINDOWS\system32\drivers\dxg.sys
Opens:                  C:\WINDOWS\system32\drivers\dxgthk.sys
Opens:                  C:\WINDOWS\system32\drivers\fdc.sys
Opens:                  C:\WINDOWS\system32\drivers\fips.sys
Opens:                  C:\WINDOWS\system32\drivers\flpydisk.sys
Opens:                  C:\WINDOWS\system32\drivers\fs_rec.sys
Opens:                  C:\WINDOWS\system32\drivers\http.sys
Opens:                  C:\WINDOWS\system32\drivers\i8042prt.sys
Opens:                  C:\WINDOWS\system32\drivers\imapi.sys
Opens:                  C:\WINDOWS\system32\drivers\ipnat.sys
Opens:                  C:\WINDOWS\system32\drivers\ipsec.sys
Opens:                  C:\WINDOWS\system32\drivers\kbdclass.sys
Opens:                  C:\WINDOWS\system32\drivers\ks.sys
Opens:                  C:\WINDOWS\system32\drivers\mnmdd.sys
Opens:                  C:\WINDOWS\system32\drivers\mouclass.sys
Opens:                  C:\WINDOWS\system32\drivers\mrxdav.sys
Opens:                  C:\WINDOWS\system32\drivers\mrxsmb.sys
Opens:                  C:\WINDOWS\system32\drivers\msfs.sys
Opens:                  C:\WINDOWS\system32\drivers\msgpc.sys
Opens:                  C:\WINDOWS\system32\drivers\mssmbios.sys
Opens:                  C:\WINDOWS\system32\drivers\ndistapi.sys
Opens:                  C:\WINDOWS\system32\drivers\ndisuio.sys
Opens:                  C:\WINDOWS\system32\drivers\ndiswan.sys
Opens:                  C:\WINDOWS\system32\drivers\ndproxy.sys
Opens:                  C:\WINDOWS\system32\drivers\netbios.sys
Opens:                  C:\WINDOWS\system32\drivers\netbt.sys
Opens:                  C:\WINDOWS\system32\drivers\npfs.sys
Opens:                  C:\WINDOWS\system32\drivers\null.sys
Opens:                  C:\WINDOWS\system32\drivers\parport.sys
Opens:                  C:\WINDOWS\system32\drivers\parvdm.sys
Opens:                  C:\WINDOWS\system32\drivers\pcntpci5.sys
Opens:                  C:\WINDOWS\system32\drivers\psched.sys
Opens:                  C:\WINDOWS\system32\drivers\ptilink.sys
Opens:                  C:\WINDOWS\system32\drivers\rasacd.sys
Opens:                  C:\WINDOWS\system32\drivers\rasl2tp.sys
Opens:                  C:\WINDOWS\system32\drivers\raspppoe.sys
Opens:                  C:\WINDOWS\system32\drivers\raspptp.sys
Opens:                  C:\WINDOWS\system32\drivers\raspti.sys
Opens:                  C:\WINDOWS\system32\drivers\rdbss.sys
Opens:                  C:\WINDOWS\system32\drivers\rdpcdd.sys
Opens:                  C:\WINDOWS\system32\drivers\rdpdr.sys
Opens:                  C:\WINDOWS\system32\drivers\rdpwd.sys
Opens:                  C:\WINDOWS\system32\drivers\redbook.sys
Opens:                  C:\WINDOWS\system32\drivers\serial.sys
Opens:                  C:\WINDOWS\system32\drivers\sfloppy.sys
Opens:                  C:\WINDOWS\system32\drivers\srv.sys
Opens:                  C:\WINDOWS\system32\drivers\swenum.sys
Opens:                  C:\WINDOWS\system32\drivers\tcpip.sys
Opens:                  C:\WINDOWS\system32\drivers\tdi.sys
Opens:                  C:\WINDOWS\system32\drivers\tdtcp.sys
Opens:                  C:\WINDOWS\system32\drivers\termdd.sys
Opens:                  C:\WINDOWS\system32\drivers\update.sys
Opens:                  C:\WINDOWS\system32\drivers\vga.sys
Opens:                  C:\WINDOWS\system32\drivers\videoprt.sys
Opens:                  C:\WINDOWS\system32\drivers\wanarp.sys
Opens:                  C:\WINDOWS\system32\dssenh.dll
Opens:                  C:\WINDOWS\system32\duser.dll
Opens:                  C:\WINDOWS\system32\eapolqec.dll
Opens:                  C:\WINDOWS\system32\eappcfg.dll
Opens:                  C:\WINDOWS\system32\eappprxy.dll
Opens:                  C:\WINDOWS\system32\els.dll
Opens:                  C:\WINDOWS\system32\en-US\ieframe.dll.mui
Opens:                  C:\WINDOWS\system32\en-US\mshtml.dll.mui
Opens:                  C:\WINDOWS\system32\en-US\urlmon.dll.mui
Opens:                  C:\WINDOWS\system32\ersvc.dll
Opens:                  C:\WINDOWS\system32\es.dll
Opens:                  C:\WINDOWS\system32\esent.dll
Opens:                  C:\WINDOWS\system32\eventlog.dll
Opens:                  C:\WINDOWS\system32\filemgmt.dll
Opens:                  C:\WINDOWS\system32\fldrclnr.dll
Opens:                  C:\WINDOWS\system32\FNTCACHE.DAT
Opens:                  C:\WINDOWS\system32\framebuf.dll
Opens:                  C:\WINDOWS\system32\freecell.exe
Opens:                  C:\WINDOWS\system32\gdi32.dll
```

```
  Opens:                 C:\WINDOWS\system32\geo.nls
  Opens:                 C:\WINDOWS\system32\GroupPolicy\gpt.ini
  Opens:                 C:\WINDOWS\system32\hnetwiz.dll
  Opens:                 C:\WINDOWS\system32\icaapi.dll
  Opens:                 C:\WINDOWS\system32\icfgnt5.dll
  Opens:                 C:\WINDOWS\system32\ieframe.dll
  Opens:                 C:\WINDOWS\system32\iepeers.dll
  Opens:                 C:\WINDOWS\system32\iertutil.dll
  Opens:                 C:\WINDOWS\system32\ieui.dll
  Opens:                 C:\WINDOWS\system32\imagehlp.dll
  Opens:                 C:\WINDOWS\system32\imgutil.dll
  Opens:                 C:\WINDOWS\system32\inetpp.dll
  Opens:                 C:\WINDOWS\system32\ipconfig.exe
  Opens:                 C:\WINDOWS\system32\iphlpapi.dll
  Opens:                 C:\WINDOWS\system32\ipnathlp.dll
  Opens:                 C:\WINDOWS\system32\ipsecsvc.dll
  Opens:                 C:\WINDOWS\system32\jscript.dll
  Opens:                 C:\WINDOWS\system32\kbdus.dll
  Opens:                 C:\WINDOWS\system32\langwrbk.dll
  Opens:                 C:\WINDOWS\system32\licdll.dll
  Opens:                 C:\WINDOWS\system32\linkinfo.dll
  Opens:                 C:\WINDOWS\system32\lmhsvc.dll
  Opens:                 C:\WINDOWS\system32\locale.nls
  Opens:                 C:\WINDOWS\system32\localspl.dll
  Opens:                 C:\WINDOWS\system32\logonui.exe
  Opens:                 C:\WINDOWS\system32\logonui.exe.manifest
  Opens:                 C:\WINDOWS\system32\lsasrv.dll
  Opens:                 C:\WINDOWS\system32\lsass.exe
  Opens:                 C:\WINDOWS\system32\lz32.dll
  Opens:                 C:\WINDOWS\system32\magnify.exe
  Opens:                 C:\WINDOWS\system32\mfc42u.dll
  Opens:                 C:\WINDOWS\system32\Microsoft\Protect\S-1-5-18\User\64e48102-28d3-4d80-
a0bc-8670c61b3123
  Opens:                 C:\WINDOWS\system32\Microsoft\Protect\S-1-5-18\User\ad629f5b-7a11-402d-
bbbd-4c66ed78de53
  Opens:                 C:\WINDOWS\system32\mlang.dll
  Opens:                 C:\WINDOWS\system32\mobsync.exe
  Opens:                 C:\WINDOWS\system32\moricons.dll
  Opens:                 C:\WINDOWS\system32\mpr.dll
  Opens:                 C:\WINDOWS\system32\msacm32.dll
  Opens:                 C:\WINDOWS\system32\mscoree.dll
  Opens:                 C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                 C:\WINDOWS\system32\msgina.dll
  Opens:                 C:\WINDOWS\system32\mshearts.exe
  Opens:                 C:\WINDOWS\system32\mshtml.dll
  Opens:                 C:\WINDOWS\system32\msi.dll
  Opens:                 C:\WINDOWS\system32\msidle.dll
  Opens:                 C:\WINDOWS\system32\msiexec.exe
  Opens:                 C:\WINDOWS\system32\msls31.dll
  Opens:                 C:\WINDOWS\system32\mspaint.exe
  Opens:                 C:\WINDOWS\system32\msprivs.dll
  Opens:                 C:\WINDOWS\system32\mstask.dll
  Opens:                 C:\WINDOWS\system32\mstlsapi.dll
  Opens:                 C:\WINDOWS\system32\mstsc.exe
  Opens:                 C:\WINDOWS\system32\msutb.dll
  Opens:                 C:\WINDOWS\system32\msvcp60.dll
  Opens:                 C:\WINDOWS\system32\msvcrt.dll
  Opens:                 C:\WINDOWS\system32\msvfw32.dll
  Opens:                 C:\WINDOWS\system32\mtxclu.dll
  Opens:                 C:\WINDOWS\system32\mycomput.dll
  Opens:                 C:\WINDOWS\system32\mydocs.dll
  Opens:                 C:\WINDOWS\system32\narrator.exe
  Opens:                 C:\WINDOWS\system32\narrhook.dll
  Opens:                 C:\WINDOWS\system32\ncobjapi.dll
  Opens:                 C:\WINDOWS\system32\nddeapi.dll
  Opens:                 C:\WINDOWS\system32\netapi32.dll
  Opens:                 C:\WINDOWS\system32\netcfgx.dll
  Opens:                 C:\WINDOWS\system32\netevent.dll
  Opens:                 C:\WINDOWS\system32\netlogon.dll
  Opens:                 C:\WINDOWS\system32\netman.dll
  Opens:                 C:\WINDOWS\system32\netmsg.dll
  Opens:                 C:\WINDOWS\system32\netshell.dll
  Opens:                 C:\WINDOWS\system32\normaliz.dll
  Opens:                 C:\WINDOWS\system32\notepad.exe
  Opens:                 C:\WINDOWS\system32\ntbackup.exe
  Opens:                 C:\WINDOWS\system32\ntdsapi.dll
  Opens:                 C:\WINDOWS\system32\ntkrnlpa.exe
  Opens:                 C:\WINDOWS\system32\ntmarta.dll
  Opens:                 C:\WINDOWS\system32\ntoskrnl.exe
  Opens:                 C:\WINDOWS\system32\ntshrui.dll
  Opens:                 C:\WINDOWS\system32\ntvdm.exe
  Opens:                 C:\WINDOWS\system32\oakley.dll
  Opens:                 C:\WINDOWS\system32\odbc32.dll
```

```
Opens:                 C:\WINDOWS\system32\odbcad32.exe
Opens:                 C:\WINDOWS\system32\odbcbcp.dll
Opens:                 C:\WINDOWS\system32\odbcint.dll
Opens:                 C:\WINDOWS\system32\ole32.dll
Opens:                 C:\WINDOWS\system32\oleacc.dll
Opens:                 C:\WINDOWS\system32\oleaccrc.dll
Opens:                 C:\WINDOWS\system32\oleaut32.dll
Opens:                 C:\WINDOWS\system32\olecli32.dll
Opens:                 C:\WINDOWS\system32\olecnv32.dll
Opens:                 C:\WINDOWS\system32\oledlg.dll
Opens:                 C:\WINDOWS\system32\olesvr32.dll
Opens:                 C:\WINDOWS\system32\olethk32.dll
Opens:                 C:\WINDOWS\system32\onex.dll
Opens:                 C:\WINDOWS\system32\oobe\actsetup\activ.htm
Opens:                 C:\WINDOWS\system32\oobe\actsetup\activsvc.htm
Opens:                 C:\WINDOWS\system32\oobe\actsetup\aregsty2.css
Opens:                 C:\WINDOWS\system32\oobe\actsetup\aregstyl.css
Opens:                 C:\WINDOWS\system32\oobe\actsetup\stgact.htm
Opens:                 C:\WINDOWS\system32\oobe\actshell.htm
Opens:                 C:\WINDOWS\system32\oobe\dialmgr.js
Opens:                 C:\WINDOWS\system32\oobe\error.js
Opens:                 C:\WINDOWS\system32\oobe\icsmgr.js
Opens:                 C:\WINDOWS\system32\oobe\images\progress.gif
Opens:                 C:\WINDOWS\system32\oobe\images\wpaback.jpg
Opens:                 C:\WINDOWS\system32\oobe\images\wpabtm.jpg
Opens:                 C:\WINDOWS\system32\oobe\images\wpaflag.jpg
Opens:                 C:\WINDOWS\system32\oobe\images\wpakey.jpg
Opens:                 C:\WINDOWS\system32\oobe\images\wpatop.jpg
Opens:                 C:\WINDOWS\system32\oobe\msobcomm.dll
Opens:                 C:\WINDOWS\system32\oobe\msobmain.dll
Opens:                 C:\WINDOWS\system32\oobe\msobshel.dll
Opens:                 C:\WINDOWS\system32\oobe\msobshel.htm
Opens:                 C:\WINDOWS\system32\oobe\msobweb.dll
Opens:                 C:\WINDOWS\system32\oobe\msoobe.exe
Opens:                 C:\WINDOWS\system32\oobe\oobeinfo.ini
Opens:                 C:\WINDOWS\system32\oobe\oobeutil.js
Opens:                 C:\WINDOWS\system32\osk.exe
Opens:                 C:\WINDOWS\system32\pdh.dll
Opens:                 C:\WINDOWS\system32\perfc009.dat
Opens:                 C:\WINDOWS\system32\perfdisk.dll
Opens:                 C:\WINDOWS\system32\perfh009.dat
Opens:                 C:\WINDOWS\system32\perfos.dll
Opens:                 C:\WINDOWS\system32\pjlmon.dll
Opens:                 C:\WINDOWS\system32\pngfilt.dll
Opens:                 C:\WINDOWS\system32\powrprof.dll
Opens:                 C:\WINDOWS\system32\profmap.dll
Opens:                 C:\WINDOWS\system32\psapi.dll
Opens:                 C:\WINDOWS\system32\psbase.dll
Opens:                 C:\WINDOWS\system32\pstorsvc.dll
Opens:                 C:\WINDOWS\system32\python27.dll
Opens:                 C:\WINDOWS\system32\pythoncom27.dll
Opens:                 C:\WINDOWS\system32\pywintypes27.dll
Opens:                 C:\WINDOWS\system32\qutil.dll
Opens:                 C:\WINDOWS\system32\raschap.dll
Opens:                 C:\WINDOWS\system32\rasdlg.dll
Opens:                 C:\WINDOWS\system32\rastls.dll
Opens:                 C:\WINDOWS\system32\rcimlby.exe
Opens:                 C:\WINDOWS\system32\rdpdd.dll
Opens:                 C:\WINDOWS\system32\rdpwsx.dll
Opens:                 C:\WINDOWS\system32\regapi.dll
Opens:                 C:\WINDOWS\system32\regsvc.dll
Opens:                 C:\WINDOWS\system32\Restore\rstrui.exe
Opens:                 C:\WINDOWS\system32\resutils.dll
Opens:                 C:\WINDOWS\system32\riched20.dll
Opens:                 C:\WINDOWS\system32\rpcrt4.dll
Opens:                 C:\WINDOWS\system32\rpcss.dll
Opens:                 C:\WINDOWS\system32\rtutils.dll
Opens:                 C:\WINDOWS\system32\rundll32.exe
Opens:                 C:\WINDOWS\system32\samsrv.dll
Opens:                 C:\WINDOWS\system32\scecli.dll
Opens:                 C:\WINDOWS\system32\scesrv.dll
Opens:                 C:\WINDOWS\system32\schannel.dll
Opens:                 C:\WINDOWS\system32\schedsvc.dll
Opens:                 C:\WINDOWS\system32\sclgntfy.dll
Opens:                 C:\WINDOWS\system32\scrrun.dll
Opens:                 C:\WINDOWS\system32\seclogon.dll
Opens:                 C:\WINDOWS\system32\secur32.dll
Opens:                 C:\WINDOWS\system32\security.dll
Opens:                 C:\WINDOWS\system32\services.exe
Opens:                 C:\WINDOWS\system32\sfc.dll
Opens:                 C:\WINDOWS\system32\sfcfiles.dll
Opens:                 C:\WINDOWS\system32\sfc_os.dll
Opens:                 C:\WINDOWS\system32\shdocvw.dll
```

```
Opens:                      C:\WINDOWS\system32\shfolder.dll
Opens:                      C:\WINDOWS\system32\shgina.dll
Opens:                      C:\WINDOWS\system32\shimeng.dll
Opens:                      C:\WINDOWS\system32\shlwapi.dll
Opens:                      C:\WINDOWS\system32\shsvcs.dll
Opens:                      C:\WINDOWS\system32\smss.exe
Opens:                      C:\WINDOWS\system32\sndrec32.exe
Opens:                      C:\WINDOWS\system32\sndvol32.exe
Opens:                      C:\WINDOWS\system32\sol.exe
Opens:                      C:\WINDOWS\system32\sortkey.nls
Opens:                      C:\WINDOWS\system32\sorttbls.nls
Opens:                      C:\WINDOWS\system32\spider.exe
Opens:                      C:\WINDOWS\system32\spoolss.dll
Opens:                      C:\WINDOWS\system32\spoolsv.exe
Opens:                      C:\WINDOWS\system32\spool\prtprocs\w32x86\filterpipelineprintproc.dll
Opens:                      C:\WINDOWS\system32\srsvc.dll
Opens:                      C:\WINDOWS\system32\srvsvc.dll
Opens:                      C:\WINDOWS\system32\ssdpapi.dll
Opens:                      C:\WINDOWS\system32\ssdpsrv.dll
Opens:                      C:\WINDOWS\system32\stdole2.tlb
Opens:                      C:\WINDOWS\system32\stobject.dll
Opens:                      C:\WINDOWS\system32\svchost.exe
Opens:                      C:\WINDOWS\system32\sxs.dll
Opens:                      C:\WINDOWS\system32\sysmon.ocx
Opens:                      C:\WINDOWS\system32\syssetup.dll
Opens:                      C:\WINDOWS\system32\tcpmon.dll
Opens:                      C:\WINDOWS\system32\termsrv.dll
Opens:                      C:\WINDOWS\system32\themeui.dll
Opens:                      C:\WINDOWS\system32\tlntsrv.exe
Opens:                      C:\WINDOWS\system32\tourstart.exe
Opens:                      C:\WINDOWS\system32\trkwks.dll
Opens:                      C:\WINDOWS\system32\tsddd.dll
Opens:                      C:\WINDOWS\system32\umandlg.dll
Opens:                      C:\WINDOWS\system32\umpnpmgr.dll
Opens:                      C:\WINDOWS\system32\unicode.nls
Opens:                      C:\WINDOWS\system32\upnp.dll
Opens:                      C:\WINDOWS\system32\url.dll
Opens:                      C:\WINDOWS\system32\urlmon.dll
Opens:                      C:\WINDOWS\system32\usbmon.dll
Opens:                      C:\WINDOWS\system32\userenv.dll
Opens:                      C:\WINDOWS\system32\userinit.exe
Opens:                      C:\WINDOWS\system32\usmt\migwiz.exe
Opens:                      C:\WINDOWS\system32\usp10.dll
Opens:                      C:\WINDOWS\system32\utilman.exe
Opens:                      C:\WINDOWS\system32\uxtheme.dll
Opens:                      C:\WINDOWS\system32\version.dll
Opens:                      C:\WINDOWS\system32\vga.dll
Opens:                      C:\WINDOWS\system32\vga256.dll
Opens:                      C:\WINDOWS\system32\vga64k.dll
Opens:                      C:\WINDOWS\system32\vssapi.dll
Opens:                      C:\WINDOWS\system32\w32time.dll
Opens:                      C:\WINDOWS\system32\watchdog.sys
Opens:                      C:\WINDOWS\system32\wbem\esscli.dll
Opens:                      C:\WINDOWS\system32\wbem\fastprox.dll
Opens:                      C:\WINDOWS\system32\wbem\framedyn.dll
Opens:                      C:\WINDOWS\system32\wbem\ncprov.dll
Opens:                      C:\WINDOWS\system32\wbem\repdrvfs.dll
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\INDEX.MAP
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\MAPPING.VER
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\MAPPING1.MAP
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\MAPPING2.MAP
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.DATA
Opens:                      C:\WINDOWS\system32\wbem\Repository\FS\OBJECTS.MAP
Opens:                      C:\WINDOWS\system32\wbem\wbemcomn.dll
Opens:                      C:\WINDOWS\system32\wbem\wbemcons.dll
Opens:                      C:\WINDOWS\system32\wbem\wbemcore.dll
Opens:                      C:\WINDOWS\system32\wbem\wbemess.dll
Opens:                      C:\WINDOWS\system32\wbem\wbemprox.dll
Opens:                      C:\WINDOWS\system32\wbem\wbemsvc.dll
Opens:                      C:\WINDOWS\system32\wbem\wmiprvsd.dll
Opens:                      C:\WINDOWS\system32\wbem\wmiprvse.exe
Opens:                      C:\WINDOWS\system32\wbem\wmisvc.dll
Opens:                      C:\WINDOWS\system32\wbem\wmiutils.dll
Opens:                      C:\WINDOWS\system32\wdigest.dll
Opens:                      C:\WINDOWS\system32\webcheck.dll
Opens:                      C:\WINDOWS\system32\webclnt.dll
Opens:                      C:\WINDOWS\system32\win32k.sys
Opens:                      C:\WINDOWS\system32\win32spl.dll
Opens:                      C:\WINDOWS\system32\WindowsLogon.manifest
Opens:                      C:\WINDOWS\system32\winhttp.dll
Opens:                      C:\WINDOWS\system32\winlogon.exe
Opens:                      C:\WINDOWS\system32\winmine.exe
```

```
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\WINDOWS\system32\winscard.dll
  Opens:                  C:\WINDOWS\system32\winspool.drv
  Opens:                  C:\WINDOWS\system32\winsrv.dll
  Opens:                  C:\WINDOWS\system32\winsta.dll
  Opens:                  C:\WINDOWS\system32\wintrust.dll
  Opens:                  C:\WINDOWS\system32\wkssvc.dll
  Opens:                  C:\WINDOWS\system32\wldap32.dll
  Opens:                  C:\WINDOWS\system32\wlnotify.dll
  Opens:                  C:\WINDOWS\system32\wmi.dll
  Opens:                  C:\WINDOWS\system32\wmp.dll
  Opens:                  C:\WINDOWS\system32\wmploc.dll
  Opens:                  C:\WINDOWS\system32\wow32.dll
  Opens:                  C:\WINDOWS\system32\wpa.dbl
  Opens:                  C:\WINDOWS\system32\wscsvc.dll
  Opens:                  C:\WINDOWS\system32\wsecedit.dll
  Opens:                  C:\WINDOWS\system32\wsock32.dll
  Opens:                  C:\WINDOWS\system32\wtsapi32.dll
  Opens:                  C:\WINDOWS\system32\wuapi.dll
  Opens:                  C:\WINDOWS\system32\wupdmgr.exe
  Opens:                  C:\WINDOWS\system32\wzcdlg.dll
  Opens:                  C:\WINDOWS\system32\wzcsapi.dll
  Opens:                  C:\WINDOWS\system32\wzcsvc.dll
  Opens:                  C:\WINDOWS\system32\xmllite.dll
  Opens:                  C:\WINDOWS\system32\xpsp1res.dll
  Opens:                  C:\WINDOWS\system32\xpsp2res.dll
  Opens:                  C:\WINDOWS\system32\xpsp3res.dll
  Opens:                  C:\WINDOWS\Tasks\SA.DAT
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca.manifest
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_d495ac4e.manifest
  Opens:                  C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83.Manifest
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-
ww_dfb54e0c.Manifest
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_5.2.2.3_x-
ww_468466a7.Manifest
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.Windows.Networking.RtcDll_6595b64144ccf1df_5.2.2.3_x-
ww_d6bd8b95.Manifest
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.Windows.Networking.RtcRes_6595b64144ccf1df_5.2.2.3_en_16a24bc0.Manifest
  Opens:
C:\WINDOWS\WinSxS\Manifests\x86_Microsoft.Windows.SystemCompatible_6595b64144ccf1df_5.1.2600.2000_x-
ww_bcc9a281.Manifest
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.1.0.Microsoft.Windows.GdiPlus_6595b64144ccf1df_x-
ww_4e8510ac\1.0.2600.5512.Policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.1.Microsoft.Windows.SystemCompatible_6595b64144ccf1df_x-
ww_a0111510\5.1.2600.2000.Policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_x-
ww_362e60dd\5.2.2.3.Policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-
ww_c7b7206f\5.2.2.3.Policy
  Opens:                  C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-
Controls_6595b64144ccf1df_x-ww_5ddad775\6.0.2600.5512.Policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-
ww_77c24773\8.0.50727.3053.policy
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-
ww_b7353f75\9.0.30729.4148.policy
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcp80.dll
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-
ww_d495ac4e\msvcr90.dll
  Opens:                  C:\$EXTEND\
  Opens:                  C:\Documents and Settings
  Opens:                  C:\Documents and Settings\Admin\Application Data
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Protect\S-1-
5-21-1757981266-507921405-1957994488-1003
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Speech
  Opens:                  C:\Documents and Settings\Admin\Application Data\Microsoft\Speech\Files
  Opens:                  C:\Documents and Settings\Admin\Application
Data\Microsoft\Speech\Files\UserLexicons
  Opens:                  C:\Documents and Settings\Admin\Favorites
  Opens:                  C:\Documents and Settings\Admin\Local Settings
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Feeds Cache
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Internet Explorer
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Application
Data\Microsoft\Windows
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\CXCXW1MR
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                  C:\Documents and Settings\Admin\My Documents
  Opens:                  C:\Documents and Settings\Admin\Start Menu
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Accessibility
  Opens:                  C:\Documents and Settings\Admin\Start
Menu\Programs\Accessories\Entertainment
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Accessories\System
Tools
  Opens:                  C:\Documents and Settings\Admin\Start Menu\Programs\Startup
  Opens:                  C:\Documents and Settings\All Users
  Opens:                  C:\Documents and Settings\All Users\Application Data
  Opens:                  C:\Documents and Settings\All Users\Application Data\Microsoft
  Opens:                  C:\Documents and Settings\All Users\Application Data\Microsoft\User
Account Pictures
  Opens:                  C:\Documents and Settings\All Users\Desktop
  Opens:                  C:\Documents and Settings\All Users\Documents
  Opens:                  C:\Documents and Settings\All Users\Start Menu
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Accessories
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Accessibility
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Communications
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\Entertainment
  Opens:                  C:\Documents and Settings\All Users\Start
Menu\Programs\Accessories\System Tools
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Administrative
Tools
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Games
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Python 2.7
  Opens:                  C:\Documents and Settings\All Users\Start Menu\Programs\Startup
  Opens:                  C:\Documents and Settings\LocalService
  Opens:                  C:\Documents and Settings\LocalService\Application Data
  Opens:                  C:\Documents and Settings\LocalService\Cookies
  Opens:                  C:\Documents and Settings\LocalService\Local Settings
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Application
Data\Microsoft
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Application
Data\Microsoft\Windows
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\History
  Opens:                  C:\Documents and Settings\LocalService\Local
Settings\History\History.IE5
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Temporary Internet
Files
  Opens:                  C:\Documents and Settings\LocalService\Local Settings\Temporary Internet
Files\Content.IE5
  Opens:                  C:\Documents and Settings\NetworkService
  Opens:                  C:\Documents and Settings\NetworkService\Application Data
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\Application Data
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\Application
Data\Microsoft
  Opens:                  C:\Documents and Settings\NetworkService\Local Settings\Application
Data\Microsoft\Windows
  Opens:                  C:\Program Files
  Opens:                  C:\Program Files\Adobe
  Opens:                  C:\Program Files\Adobe\Reader 9.0
  Opens:                  C:\Program Files\Adobe\Reader 9.0\Reader
  Opens:                 C:\Program Files\Common Files
  Opens:                 C:\Program Files\Common Files\Adobe
  Opens:                 C:\Program Files\Common Files\Adobe\Acrobat
  Opens:                 C:\Program Files\Common Files\Adobe\Acrobat\ActiveX
  Opens:                 C:\Program Files\Common Files\Adobe\ARM
  Opens:                 C:\Program Files\Common Files\Adobe\ARM\1.0
  Opens:                 C:\Program Files\Common Files\Java
  Opens:                 C:\Program Files\Common Files\Java\Java Update
  Opens:                 C:\Program Files\Common Files\Microsoft Shared
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\MSInfo
  Opens:                 C:\Program Files\Common Files\Microsoft Shared\Speech
  Opens:                 C:\Program Files\Common Files\SpeechEngines
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\Lexicon
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\Lexicon\1033
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS
  Opens:                 C:\Program Files\Common Files\SpeechEngines\Microsoft\TTS\1033
  Opens:                 C:\Program Files\Internet Explorer
  Opens:                 C:\Program Files\Java
  Opens:                 C:\Program Files\Java\jre7
  Opens:                 C:\Program Files\Java\jre7\lib\deploy
  Opens:                 C:\Program Files\Java\jre7\lib\deploy\jqs
  Opens:                 C:\Program Files\Messenger
  Opens:                 C:\Program Files\Microsoft Office
  Opens:                 C:\Program Files\Movie Maker
  Opens:                 C:\Program Files\MSN Gaming Zone
  Opens:                 C:\Program Files\MSN Gaming Zone\Windows
  Opens:                 C:\Program Files\MSN
  Opens:                 C:\Program Files\MSN\MSNCoreFiles
  Opens:                 C:\Program Files\MSN\MSNCoreFiles\Install
  Opens:                 C:\Program Files\Outlook Express
  Opens:                 C:\Program Files\Windows Media Player
  Opens:                 C:\Program Files\Windows NT
  Opens:                 C:\Program Files\Windows NT\Accessories
  Opens:                 C:\Program Files\Windows NT\Pinball
  Opens:                 C:\System Volume Information
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP22
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP24
  Opens:                 C:\System Volume Information\_restore{DFC4753E-A69F-4404-9702-
0D4648AC633B}\RP25
  Opens:                 C:\WINDOWS
  Opens:                 C:\WINDOWS\AppPatch
  Opens:                 C:\WINDOWS\Debug
  Opens:                 C:\WINDOWS\Debug\UserMode
  Opens:                 C:\WINDOWS\Fonts
  Opens:                 C:\WINDOWS\ime
  Opens:                 C:\WINDOWS\Installer
  Opens:                 C:\WINDOWS\Installer\{90850409-6000-11D3-8CFE-0150048383C9}
  Opens:                 C:\WINDOWS\Installer\{95120000-003F-0409-0000-0000000FF1CE}
  Opens:                 C:\WINDOWS\Installer\{95140000-00AF-0409-0000-0000000FF1CE}
  Opens:                 C:\WINDOWS\Installer\{AC76BA86-7AD7-1033-7B44-A93000000001}
  Opens:                 C:\WINDOWS\Installer\{C3CC4DF5-39A5-4027-B136-2B3E1F5AB6E2}
  Opens:                 C:\WINDOWS\Microsoft.NET
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework
  Opens:                 C:\WINDOWS\pchealth
  Opens:                 C:\WINDOWS\pchealth\helpctr
  Opens:                 C:\WINDOWS\pchealth\helpctr\binaries
  Opens:                 C:\WINDOWS\Prefetch
  Opens:                 C:\WINDOWS\Registration
  Opens:                 C:\WINDOWS\Resources
  Opens:                 C:\WINDOWS\Resources\Themes
  Opens:                 C:\WINDOWS\Resources\Themes\Luna
  Opens:                 C:\WINDOWS\system32
  Opens:                 C:\WINDOWS\system32\config
  Opens:                 C:\WINDOWS\system32\drivers
  Opens:                 C:\WINDOWS\system32\drivers\etc
  Opens:                 C:\WINDOWS\system32\en-US
  Opens:                 C:\WINDOWS\system32\GroupPolicy
  Opens:                 C:\WINDOWS\system32\Microsoft
  Opens:                 C:\WINDOWS\system32\Microsoft\Protect
  Opens:                 C:\WINDOWS\system32\Microsoft\Protect\S-1-5-18
  Opens:                 C:\WINDOWS\system32\Microsoft\Protect\S-1-5-18\User
  Opens:                 C:\WINDOWS\system32\oobe
  Opens:                 C:\WINDOWS\system32\oobe\actsetup
  Opens:                 C:\WINDOWS\system32\oobe\images
  Opens:                 C:\WINDOWS\system32\Restore
  Opens:                 C:\WINDOWS\system32\spool
  Opens:                 C:\WINDOWS\system32\spool\drivers
  Opens:                 C:\WINDOWS\system32\spool\drivers\w32x86
  Opens:                  C:\WINDOWS\system32\spool\prtprocs
  Opens:                  C:\WINDOWS\system32\spool\prtprocs\w32x86
  Opens:                  C:\WINDOWS\system32\usmt
  Opens:                  C:\WINDOWS\system32\wbem
  Opens:                  C:\WINDOWS\system32\wbem\Logs
  Opens:                  C:\WINDOWS\system32\wbem\Repository
  Opens:                  C:\WINDOWS\system32\wbem\Repository\FS
  Opens:                  C:\WINDOWS\Tasks
  Opens:                  C:\WINDOWS\WinSxS
  Opens:                  C:\WINDOWS\WinSxS\Manifests
  Opens:                  C:\WINDOWS\WinSxS\Policies
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.1.0.Microsoft.Windows.GdiPlus_6595b64144ccf1df_x-
ww_4e8510ac
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.1.Microsoft.Windows.SystemCompatible_6595b64144ccf1df_x-
ww_a0111510
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Dxmrtp_6595b64144ccf1df_x-
ww_362e60dd
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.5.2.Microsoft.Windows.Networking.Rtcdll_6595b64144ccf1df_x-
ww_c7b7206f
  Opens:                  C:\WINDOWS\WinSxS\Policies\x86_policy.6.0.Microsoft.Windows.Common-
Controls_6595b64144ccf1df_x-ww_5ddad775
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.8.0.Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_x-ww_77c24773
  Opens:
C:\WINDOWS\WinSxS\Policies\x86_policy.9.0.Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_x-ww_b7353f75
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
  Opens:                  C:\WINDOWS\Prefetch\RUNDLL32.EXE-18273726.pf
  Opens:                  C:\WINDOWS\system32\config\system
  Opens:                  C:\WINDOWS\system32\timedate.cpl
  Opens:                  C:\WINDOWS\Prefetch\PYTHONW.EXE-1A630664.pf
  Opens:                  C:\TMP1Q1YGB.PYW
  Opens:                  C:\WINDOWS\Prefetch\REG.EXE-0D2A95F7.pf
  Opens:                  C:\WINDOWS\system32\reg.exe
  Opens:                  C:\WINDOWS\Prefetch\SC.EXE-012262AF.pf
  Opens:                  C:\WINDOWS\system32\sc.exe
  Opens:                  C:\WINDOWS\Prefetch\IVM-SERVICE.EXE-074ABCAF.pf
  Opens:                  C:\WINDOWS\Prefetch\UNSECAPP.EXE-1A95A33B.pf
  Opens:                  C:\WINDOWS\system32\wbem\unsecapp.exe
  Opens:                  C:\WINDOWS\TEMP\SPYEYE_INJECTOR.EXE
  Opens:                  C:\WINDOWS\Prefetch\WMIPRVSE.EXE-28F301A9.pf
  Opens:                  C:\WINDOWS\Prefetch\PARANORMAL.EXE-05B653A9.pf
  Opens:                  C:\WINDOWS\Prefetch\CALC.EXE-02CD573A.pf
  Writes to:              C:\WinOldFileq\83A49421643.exe
  Writes to:              C:\WinOldFileq\B20776D7F8FB639
  Writes to:              C:\WINDOWS\system32\wbem\Logs\wbemess.log
  Writes to:              C:\Documents and Settings\Admin\Cookies\admin@microsoft[2].txt
  Writes to:              C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
  Writes to:              C:\WINDOWS\Prefetch\NTOSBOOT-B00DFAAD.pf
  Writes to:              C:\WINDOWS\Prefetch\RUNDLL32.EXE-18273726.pf
  Writes to:              C:\WINDOWS\Prefetch\PYTHONW.EXE-1A630664.pf
  Writes to:              C:\WINDOWS\Prefetch\REG.EXE-0D2A95F7.pf
  Writes to:              C:\WINDOWS\Prefetch\SC.EXE-012262AF.pf
  Writes to:              C:\WINDOWS\Prefetch\IVM-SERVICE.EXE-074ABCAF.pf
  Writes to:              C:\WINDOWS\Prefetch\83A49421643.EXE-1FEF9BA6.pf
  Writes to:              C:\WINDOWS\Prefetch\UNSECAPP.EXE-1A95A33B.pf
  Writes to:              C:\WINDOWS\Prefetch\SPYEYE_INJECTOR.EXE-255B270C.pf
  Writes to:              C:\WINDOWS\Prefetch\WMIPRVSE.EXE-28F301A9.pf
  Writes to:              C:\WINDOWS\Prefetch\PARANORMAL.EXE-05B653A9.pf
  Writes to:              C:\WINDOWS\Prefetch\CALC.EXE-02CD573A.pf
  Reads from:             C:\WINDOWS\system32\ntdll.dll
  Reads from:             C:\WINDOWS\Temp\spyeye_injector.exe
  Reads from:             C:\WinOldFileq\B20776D7F8FB639
  Reads from:             C:\WINDOWS\system32\user32.dll
  Reads from:             C:\WINDOWS\system32\wininet.dll
  Reads from:             C:\WinOldFileq\83A49421643.exe
  Reads from:             C:\WINDOWS\system32\ws2_32.dll
  Reads from:             C:\WINDOWS\system32\advapi32.dll
  Reads from:             C:\WINDOWS\system32\crypt32.dll
  Reads from:             C:\AUTOEXEC.BAT
  Reads from:             C:\WINDOWS\system32\wbem\Repository\$WinMgmt.CFG
  Reads from:             C:\WINDOWS\system32\sens.dll
  Reads from:             C:\WINDOWS\system32\calc.exe
  Reads from:             C:\WINDOWS\win.ini
  Reads from:             C:\Program Files\Java\jre7\lib\content-types.properties
  Reads from:             C:\Program Files\Java\jre7\lib\deploy.jar
  Reads from:             C:\Program Files\Java\jre7\lib\ext\dnsns.jar
  Reads from:            C:\Program Files\Java\jre7\lib\ext\localedata.jar
  Reads from:            C:\Program Files\Java\jre7\lib\fontconfig.bfc
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaBrightDemiBold.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaBrightDemiItalic.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaBrightItalic.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaBrightRegular.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaSansDemiBold.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaSansRegular.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaTypewriterBold.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\fonts\LucidaTypewriterRegular.ttf
  Reads from:            C:\Program Files\Java\jre7\lib\javaws.jar
  Reads from:            C:\Program Files\Java\jre7\lib\logging.properties
  Reads from:            C:\Program Files\Java\jre7\lib\meta-index
  Reads from:            C:\Program Files\Java\jre7\lib\net.properties
  Reads from:            C:\Program Files\Java\jre7\lib\plugin.jar
  Reads from:            C:\Program Files\Java\jre7\lib\resources.jar
  Reads from:            C:\Program Files\Java\jre7\lib\rt.jar
  Reads from:            C:\Program Files\Java\jre7\lib\security\blacklist
  Reads from:            C:\Program Files\Java\jre7\lib\security\java.policy
  Reads from:            C:\Program Files\Java\jre7\lib\security\java.security
  Reads from:            C:\Program Files\Java\jre7\lib\security\javaws.policy
  Reads from:            C:\Program Files\Java\jre7\lib\tzmappings
  Reads from:            C:\Program Files\Java\jre7\lib\zi\GMT
  Reads from:            C:\WINDOWS\system32\rsaenh.dll
  Reads from:            C:\Documents and Settings\Admin\Cookies\admin@www.microsoft[2].txt
  Reads from:            C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
  Deletes:               C:\WINDOWS\Temp\spyeye_injector.exe
  Deletes:               C:\Documents and Settings\Admin\Cookies\admin@microsoft[1].txt
  Deletes:               C:\Documents and Settings\Admin\Cookies\admin@microsoft[2].txt
```

Network Events

```
  DNS query:             alexeyartemov.com
  DNS query:             www.microsoft.com
  DNS response:          alexeyartemov.com ⇒ 198.105.244.11
  DNS response:          alexeyartemov.com ⇒ 104.239.213.7
  DNS response:          e10088.dspb.akamaiedge.net ⇒ 23.7.35.22
  DNS response:          e10088.dspb.akamaiedge.net ⇒ 184.86.231.62
  Connects to:           88.198.13.147:443
  Connects to:           104.239.213.7:80
  Connects to:           23.7.35.22:80
  Sends data to:         8.8.8.8:53
  Sends data to:         4.2.2.1:53
  Sends data to:         88.198.13.147:443
  Sends data to:         alexeyartemov.com:80 (104.239.213.7)
  Sends data to:         e10088.dspb.akamaiedge.net:80 (23.7.35.22)
  Receives data from:    8.8.8.8:53
  Receives data from:    4.2.2.1:53
  Receives data from:    alexeyartemov.com:80 (104.239.213.7)
  Receives data from:    0.0.0.0:0
  Receives data from:    e10088.dspb.akamaiedge.net:80 (23.7.35.22)
```

Windows Registry Events

```
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:           HKCU\software\microsoft\windows\currentversion\run
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Creates key:           HKCU\software\microsoft\internet explorer\phishingfilter
  Creates key:           HKCU\software\microsoft\internet explorer\recovery
  Creates key:           HKLM\software\classes
  Creates key:           HKU\.default\software\microsoft\windows\currentversion\internet settings
  Creates key:           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:           HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:           HKCU\software\microsoft\systemcertificates\my
  Creates key:           HKCU\software\microsoft\windows nt\currentversion\winlogon
  Creates key:           HKCU\software\microsoft windows
  Creates key:           HKLM\software\microsoft\wbem\cimom
  Creates key:           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:           HKLM\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:           HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\connections
  Creates key:              HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:              HKCU\software\microsoft\windows nt\currentversion\network\location
awareness
  Creates key:              HKLM\system\currentcontrolset\services\netbt\parameters
  Creates key:
HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities\mediamodes
  Creates key:              HKLM\software\microsoft\windows\currentversion\h323tsp
  Creates key:              HKCU\sessioninformation
  Creates key:              HKLM\system\currentcontrolset\services\eventlog\application\microsoft
h.323 telephony service provider
  Creates key:              HKLM\system\currentcontrolset\control\deviceclasses
  Creates key:              HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history
  Creates key:              HKLM\system\currentcontrolset\services\sharedaccess\epoch
  Deletes value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Deletes value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Deletes value:            HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\spyeye_injector.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpr.dll
  Opens key:                HKLM\system\currentcontrolset\control\networkprovider\hworder
  Opens key:                HKLM\system\currentcontrolset
  Opens key:                HKLM\system\currentcontrolset\services\rdpnp\networkprovider
  Opens key:                HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider
  Opens key:                HKLM\system\currentcontrolset\services\webclient\networkprovider
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\drprov.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netui0.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netrap.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netui1.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntlanman.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\davclnt.dll
  Opens key:                HKCU\network
  Opens key:                HKLM\system\wpa\tabletpc
  Opens key:                HKLM\system\wpa\mediacenter
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\83a49421643.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\83a49421643.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\user32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\protocols\name-space handler\
  Opens key:                HKCR\protocols\name-space handler
  Opens key:                HKCU\software\classes\protocols\name-space handler
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\system\currentcontrolset\control\wmi\security
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msimg32.dll
```

```
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:               HKLM\system\setup
  Opens key:               HKLM\software\microsoft\internet explorer
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet settings\user
agent
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings\user
agent
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\ua tokens
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\pre platform
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\pre platform
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet settings\user
agent\post platform
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent\post platform
  Opens key:               HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_browser_emulation
  Opens key:               HKLM\software\policies\microsoft\internet explorer\main
  Opens key:               HKU\.default\software\policies\microsoft\control panel\desktop
  Opens key:               HKU\.default\control panel\desktop
  Opens key:               HKCR\protocols\name-space handler\
  Opens key:               HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:               HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:               HKU\.default\software\policies\microsoft\internet
explorer\main\featurecontrol
  Opens key:               HKU\.default\software\microsoft\internet explorer\main\featurecontrol
  Opens key:               HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:               HKU\.default\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:               HKU\.default\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:               HKLM\security\policy
  Opens key:               HKLM\security\policy\secdesc
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:               HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:                 HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:                HKLM\sam\sam\domains\account\groups\000003eb
  Opens key:                HKLM\sam\sam\domains\account\aliases\000003eb
  Opens key:                HKLM\sam\sam\domains\account\users\000003eb
  Opens key:                HKLM\software\microsoft\cryptography\oid
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype 0
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\#16
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype
0\certdllopenstoreprov\ldap
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype 1
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype
1\certdllopenstoreprov
  Opens key:                HKCU\software\microsoft\systemcertificates\my\physicalstores
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:                HKCU\environment
  Opens key:                HKCU\volatile environment
  Opens key:                HKCU\software\microsoft\systemcertificates\my
  Opens key:                HKCU\software\microsoft\systemcertificates\my\
  Opens key:                HKCU\software\microsoft\systemcertificates\my\certificates
  Opens key:                HKCU\software\microsoft\systemcertificates\my\crls
  Opens key:                HKCU\software\microsoft\systemcertificates\my\ctls
  Opens key:                HKCU\software\microsoft\systemcertificates\my\keys
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\treatas
  Opens key:                HKCR\
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserver32
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserverx86
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\localserver32
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprochandler32
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprochandlerx86
  Opens key:                HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\localserver
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\treatas
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserver32
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserverx86
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\localserver32
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprochandler32
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprochandlerx86
  Opens key:                HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\rasapi32.dll
  Opens key:                HKLM\software\microsoft\tracing\rasapi32
  Opens key:                HKLM\system\currentcontrolset\services
  Opens key:                HKLM\system\currentcontrolset\services\tapisrv
  Opens key:                HKLM\system\currentcontrolset\services\tapisrv\parameters
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapisrv.dll
  Opens key:                HKLM\software\microsoft\tracing\tapisrv
  Opens key:                HKLM\system\currentcontrolset\control\productoptions
  Opens key:                HKLM\software\policies\microsoft\system\dnsclient
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKLM\software\microsoft\windows\currentversion\telephony\server
  Opens key:                HKLM\system\currentcontrolset\services\rasman
  Opens key:                HKLM\system\currentcontrolset\services\rasman\parameters
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winipsec.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasmans.dll
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\treatas
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserverx86
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\localserver32
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandler32
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprochandlerx86
  Opens key:                HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\localserver
  Opens key:                HKLM\system\currentcontrolset\control\network
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\treatas
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi
  Opens key:                HKU\.default\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserverx86
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\localserver32
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandler32
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprochandlerx86
  Opens key:                HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\localserver
  Opens key:                HKCR\appid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\treatas
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserverx86
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\localserver32
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprochandler32
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprochandlerx86
  Opens key:                HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\localserver
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\treatas
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserver32
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprocserverx86
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\localserver32
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandler32
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\inprochandlerx86
  Opens key:                HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}\localserver
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi
  Opens key:                HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings\http
filters\rpa
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces
  Opens key:                HKLM\system\currentcontrolset\services\tcpip
  Opens key:                HKU\s-1-5-18_classes
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\adapters
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:
HKLM\system\currentcontrolset\services\dhcp\configurations\alternate_{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi
  Opens key:                HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                HKLM\software\policies\microsoft\internet explorer\security
  Opens key:                HKLM\system\currentcontrolset\services\netbt
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-
abe3-c7d49d7cecdc}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rastapi.dll
  Opens key:                HKLM\software\microsoft\tracing\rastapi
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\treatas
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserverx86
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\localserver32
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandler32
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprochandlerx86
  Opens key:                HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\localserver
  Opens key:                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\treatas
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserverx86
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\localserver32
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprochandler32
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprochandlerx86
  Opens key:                HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\localserver
  Opens key:                HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib
  Opens key:                HKCR\typelib
  Opens key:                HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}
  Opens key:                HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0
  Opens key:                HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0
  Opens key:                HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32
  Opens key:                HKLM\system\currentcontrolset\services\eventlog\system
  Opens key:                HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}
  Opens key:                HKLM\system\currentcontrolset\services\eventlog\system\service control
manager
  Opens key:                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{005ea477-f098-4d38-a3c2-efb77570be00}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                HKLM\software\microsoft\tracing\tapi32
  Opens key:                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{1639c72a-1a0a-47a4-921d-ee4a54fd909e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{66df4d2a-d6c8-4cc8-98ce-d41df97bc4c0}-{00000000-0000-0000-0000-
```

```
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{6cec9440-b380-4cb9-b34e-976dcb71c997}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{9242f92e-51ec-43bc-bc55-a2114102e8d0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{c46fb167-8b94-46b1-be86-be941a22332c}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                 HKLM\system\currentcontrolset\services\vxd\mstcp
  Opens key:                 HKLM\system\currentcontrolset\control\computername\computername
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adsldpc.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\activeds.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mprapi.dll
  Opens key:
HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities
  Opens key:                 HKLM\software\microsoft\windows\currentversion\telephony\providers
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uniplat.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\unimdm.tsp
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{df286e4f-26fb-4de8-88ec-f5ad9ebb2b76}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f18496b7-574d-425c-8b5e-f6f7bff87350}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}\publisherproperties
  Opens key:                 HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}\subscriberproperties
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kmddsp.tsp
  Opens key:                 HKLM\software\microsoft\tracing\kmddsp
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ndptsp.tsp
  Opens key:                 HKLM\software\microsoft\tracing\ndptsp
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ipconf.tsp
  Opens key:                 HKLM\software\microsoft\tracing\conftsp
  Opens key:                 HKCU\software\classes\applications\calc.exe
  Opens key:                 HKCR\applications\calc.exe
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\h323.tsp
  Opens key:                 HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
  Opens key:                 HKLM\system\currentcontrolset\services\eventlog\application
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hid.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hidphone.tsp
  Opens key:                 HKLM\system\currentcontrolset\control\deviceclasses\{4d1e55b2-f16f-11cf-
88cb-001111000030}
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003
  Opens key:                 HKLM\software\microsoft\ctf\tip\
  Opens key:                 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004
  Opens key:                 HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
```

```
08002be10318}\0005
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
  Opens key:                HKLM\system\currentcontrolset\control\minint
  Opens key:                HKLM\system\currentcontrolset\services\remoteaccess
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007
  Opens key:                HKLM\system\currentcontrolset\services\nbf\linkage
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntlsapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasppp.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cryptdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kerberos.dll
  Opens key:                HKLM\system\currentcontrolset\services\rasman\parameters\quarantine
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasqec.dll
  Opens key:                HKLM\software\microsoft\tracing\rasqec
  Opens key:                HKLM\software\microsoft\tracing\rasman
  Opens key:                HKLM\software\microsoft\tracing\ppp
  Opens key:                HKLM\software\microsoft\tracing\bap
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols
  Opens key:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\chap
  Opens key:                HKLM\software\microsoft\tracing\rasspap
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\spap
  Opens key:                HKLM\software\microsoft\tracing\raspap
  Opens key:                HKLM\software\microsoft\tracing\raseap
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\eap
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\eap\13
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\eap\25
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\eap\26
  Opens key:                HKLM\system\currentcontrolset\services\rasman\ppp\eap\4
  Opens key:                HKLM\software\microsoft\tracing\rasccp
  Opens key:                HKLM\software\microsoft\tracing\rasbacp
  Opens key:                HKLM\software\microsoft\tracing\rasiphlp
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
  Opens key:                HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters
  Opens key:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{4fe87b73-b12e-47d6-
82c4-fb0d4cf73262}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}
  Opens key:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{cac79791-bd6d-4f3e-
bcad-e3686652faee}
  Opens key:                HKLM\software\microsoft\tracing\rasipcp
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:                HKLM\system\wpa\pnp
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\awt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jvm.dll
  Opens key:                HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dcpr.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\deploy.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fontmanager.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\java.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\javaw.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jp2native.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jpeg.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\net.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\nio.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\verify.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\zip.dll
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation
  Opens key:                HKCU\appevents\schemes\apps\.default\systemnotification\.current
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:                HKCU\software\microsoft\internet explorer\ietld\lowmic
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\p3p\history\microsoft.com
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder]
  Queries value:            HKLM\system\currentcontrolset\services\rdpnp\networkprovider[name]
  Queries value:            HKLM\system\currentcontrolset\services\rdpnp\networkprovider[class]
  Queries value:
HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[class]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[providerpath]
  Queries value:            HKLM\system\currentcontrolset\services\webclient\networkprovider[name]
  Queries value:            HKLM\system\currentcontrolset\services\webclient\networkprovider[class]
  Queries value:
HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters[sort hyphens]
  Queries value:            HKLM\system\wpa\mediacenter[installed]
  Queries value:
```

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[83a49421643]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[83a49421643]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:              HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:              HKCR\interface[interfacehelperdisableall]
  Queries value:              HKCR\interface[interfacehelperdisableallforole32]
  Queries value:              HKCR\interface[interfacehelperdisabletypelib]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:              HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:              HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[83a49421643.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
  Queries value:              HKLM\system\setup[systemsetupinprogress]
  Queries value:              HKLM\software\microsoft\internet explorer[version]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[compatible]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[version]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet settings[user
agent]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\user agent[platform]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value:              HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
  Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
  Queries value:              HKU\.default\control panel\desktop[multiuilanguageid]
  Queries value:              HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_protocol_lockdown[lsass.exe]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value:              HKLM\security\policy\secdesc[]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[explorer.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
```

```
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value:              HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:              HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:              HKLM\sam\sam\domains\account\users\000003eb[v]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Queries value:              HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:              HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:              HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[winlogon.exe]
  Queries value:              HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:              HKLM\software\microsoft\wbem\cimom[log file max size]
  Queries value:              HKLM\software\microsoft\com3[regdbversion]
  Queries value:              HKCR\clsid\{4fa18276-912a-11d1-ad9b-
00c04fd8fdff}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}\inprocserver32[]
  Queries value:              HKCR\clsid\{4fa18276-912a-11d1-ad9b-00c04fd8fdff}[appid]
  Queries value:              HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-
5e7582d8c9fa}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}\inprocserver32[]
  Queries value:              HKCR\clsid\{cf4cc405-e2c5-4ddd-b3ce-5e7582d8c9fa}[appid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Queries value:              HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:              HKLM\software\microsoft\tracing\netshell[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\netshell[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\netshell[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\netshell[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\netshell[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\netshell[filedirectory]
  Queries value:              HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
  Queries value:              HKLM\system\currentcontrolset\services\tapisrv\parameters[servicedll]
  Queries value:              HKLM\system\currentcontrolset\services\tapisrv\parameters[servicemain]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[enabledebuggertracing]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\tapisrv[filedirectory]
  Queries value:              HKLM\software\microsoft\tracing\wzctrace[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\wzctrace[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\wzctrace[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\wzctrace[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\wzctrace[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\wzctrace[filedirectory]
  Queries value:              HKLM\software\microsoft\tracing\eapol[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\eapol[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\eapol[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\eapol[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\eapol[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\eapol[filedirectory]
  Queries value:              HKLM\software\microsoft\tracing\eapolqec[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\eapolqec[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\eapolqec[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\eapolqec[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\eapolqec[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\eapolqec[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\eapolqeccb[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\eapolqeccb[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\eapolqeccb[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\eapolqeccb[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\eapolqeccb[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\eapolqeccb[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\svchost_rastls[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\svchost_rastls[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\svchost_rastls[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\svchost_rastls[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\svchost_rastls[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\svchost_rastls[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\svchost_raschap[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\svchost_raschap[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\svchost_raschap[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\svchost_raschap[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\svchost_raschap[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\svchost_raschap[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\oneexsup[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\oneexsup[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\oneexsup[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\oneexsup[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\oneexsup[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\oneexsup[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\wlpolicy[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\wlpolicy[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\wlpolicy[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\wlpolicy[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\wlpolicy[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\wlpolicy[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\ipnathlp[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\ipnathlp[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\ipnathlp[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\ipnathlp[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\ipnathlp[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\ipnathlp[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\dot3api[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\dot3api[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\dot3api[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\dot3api[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\dot3api[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\dot3api[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\netman[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\netman[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\netman[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\netman[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\netman[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\netman[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\rasdlg[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasdlg[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasdlg[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasdlg[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasdlg[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasdlg[filedirectory]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapisrvwaithint]
  Queries value:            HKLM\software\microsoft\windows\currentversion\telephony[min]
  Queries value:            HKLM\software\microsoft\windows\currentversion\telephony[tapiscpttl]
  Queries value:            HKLM\software\microsoft\windows\currentversion\telephony[max]
  Queries value:            HKLM\software\microsoft\windows\currentversion\telephony[rpctimeout]
  Queries value:            HKLM\software\microsoft\windows\currentversion\telephony[domainname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapisrvnumhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\tapisrv\parameters[servicedllunloadonstop]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\parameters[servicedll]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\parameters[servicemain]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[allowexternalcallers]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\parameters[prohibitipsec]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[ipoutlowwatermark]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[ipouthighwatermark]
  Queries value:            HKCR\clsid\{5b035261-40f9-11d1-aaec-
00805fc1270e}\inprocserver32[inprocserver32]
```

```
  Queries value:               HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}\inprocserver32[]
  Queries value:               HKCR\clsid\{5b035261-40f9-11d1-aaec-00805fc1270e}[appid]
  Queries value:               HKLM\system\currentcontrolset\control\network[config]
  Queries value:               HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}[description]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:               HKCR\clsid\{d5978620-5b9f-11d1-8dd2-
00aa004abd5e}\inprocserver32[inprocserver32]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[clsid]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[service]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[coservices]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[bindform]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi[helptext]
  Queries value:
HKU\.default\software\microsoft\windows\shellnoroam\muicache[@netcfgx.dll,-50001]
  Queries value:               HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}\inprocserver32[]
  Queries value:               HKCR\clsid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[appid]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[lowerrange]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[lowerexclude]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[upperrange]
  Queries value:               HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{b7d3b707-8bc4-489e-84f0-d92eb38c0674}\ndi\interfaces[filtermediatypes]
  Queries value:               HKCR\appid\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}[dllsurrogate]
  Queries value:               HKCR\clsid\{a907657f-6fdf-11d0-8efb-
00c04fd912b2}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{d5978620-5b9f-11d1-8dd2-
00aa004abd5e}\inprocserver32[threadingmodel]
  Queries value:               HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}\inprocserver32[]
  Queries value:               HKCR\clsid\{a907657f-6fdf-11d0-8efb-00c04fd912b2}[appid]
  Queries value:               HKCR\clsid\{a907657f-6fdf-11d0-8efb-
00c04fd912b2}\inprocserver32[threadingmodel]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[description]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[clsid]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[service]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[coservices]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[bindform]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi[helptext]
  Queries value:               HKCR\clsid\{1be1f766-5536-11d1-b726-00c04fb926af}[appid]
  Queries value:               HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[dllsurrogate]
  Queries value:               HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[localservice]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[lowerrange]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[lowerexclude]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[upperrange]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001\ndi\interfaces[filtermediatypes]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008[description]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[clsid]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[service]
  Queries value:               HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[coservices]
  Queries value:             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[bindform]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[serviceparameters]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[runas]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[activateatstorage]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[launchpermission]
  Queries value:             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi[helptext]
  Queries value:             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces[lowerrange]
  Queries value:             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces[lowerexclude]
  Queries value:             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces[upperrange]
  Queries value:             HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0008\ndi\interfaces[filtermediatypes]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[svchost.exe]
  Queries value:             HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[explorer.exe]
  Queries value:             HKLM\software\microsoft\ole[legacyauthenticationlevel]
  Queries value:             HKLM\software\microsoft\ole[legacyimpersonationlevel]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[authenticationlevel]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[remoteservername]
  Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[srptrustlevel]
  Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters[nameserver]
  Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters[ipenablerouter]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableicmpredirect]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[deadgwdetectdefault]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dontadddefaultgatewaydefault]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enablesecurityfilters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[numinterfaces]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[ipinterfaces]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipaddress]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[subnetmask]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[defaultgateway]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[defaultgatewaymetric]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[interfacemetric]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[tcpallowedports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[udpallowedports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[rawipallowedprotocols]
```

```
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[activeconfigurations]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}[description]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[clsid]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[service]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[coservices]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[bindform]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi[helptext]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[lowerrange]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[lowerexclude]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[upperrange]
   Queries value:             HKLM\system\currentcontrolset\control\network\{4d36e975-e325-11ce-bfc1-
08002be10318}\{61eab4e1-adba-45df-86af-11c0d7f92321}\ndi\interfaces[filtermediatypes]
   Queries value:             HKCR\appid\{1be1f766-5536-11d1-b726-00c04fb926af}[debugsurrogate]
   Queries value:             HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Queries value:             HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
   Queries value:             HKLM\system\currentcontrolset\services\netbt\parameters[enablelmhosts]
   Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-
abe3-c7d49d7cecdc}[nameserverlist]
   Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{16325b0b-4636-4303-
abe3-c7d49d7cecdc}[netbiosoptions]
   Queries value:             HKLM\system\currentcontrolset\services\rasman\parameters[medias]
   Queries value:             HKLM\software\microsoft\tracing\rastapi[enablefiletracing]
   Queries value:             HKLM\software\microsoft\tracing\rastapi[filetracingmask]
   Queries value:             HKLM\software\microsoft\tracing\rastapi[enableconsoletracing]
   Queries value:             HKLM\software\microsoft\tracing\rastapi[consoletracingmask]
   Queries value:             HKLM\software\microsoft\tracing\rastapi[maxfilesize]
   Queries value:             HKLM\software\microsoft\tracing\rastapi[filedirectory]
   Queries value:             HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-
00c04fb926af}\inprocserver32[inprocserver32]
   Queries value:             HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}\inprocserver32[]
   Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
   Queries value:             HKCR\clsid\{64b8f404-a4ae-11d1-b7b6-00c04fb926af}[appid]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassname]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[ownersid]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[firinginterfaceiid]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[customconfigclsid]
   Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[description]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[typelib]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[multiinterfacepublisherfilterclsid]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowinprocactivation]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[fireinparallel]
   Queries value:             HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclasspartitionid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassapplicationid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[parallelfiringtimeout]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuserinprocactivation]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:              HKCR\clsid\{1108be51-f58a-4cda-bb99-
7a0227d11d5e}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}\inprocserver32[]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowperuseractivateasactivator]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\eventclasses\{d5978620-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[allowperusermoniker]
   Queries value:              HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[]
   Queries value:              HKCR\interface\{d597bab1-5b9f-11d1-8dd2-00aa004abd5e}\typelib[version]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:              HKCR\typelib\{d597deed-5b9f-11d1-8dd2-00aa004abd5e}\2.0\0\win32[]
   Queries value:              HKCR\clsid\{1108be51-f58a-4cda-bb99-7a0227d11d5e}[appid]
   Queries value:              HKLM\system\currentcontrolset\services\eventlog\system[primarymodule]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:              HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperdisabletypelib]
   Queries value:              HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperdisableall]
   Queries value:              HKCR\interface\{d597bab1-5b9f-11d1-8dd2-
00aa004abd5e}[interfacehelperuser]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:              HKLM\system\currentcontrolset\services\eventlog\system[eventmessagefile]
   Queries value:              HKLM\system\currentcontrolset\services\eventlog\system\service control
manager[categorymessagefile]
   Queries value:              HKLM\system\currentcontrolset\services\eventlog\system\service control
manager[parametermessagefile]
   Queries value:              HKLM\system\currentcontrolset\services\eventlog\system\service control
manager[eventmessagefile]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{d789ab02-5b9f-11d1-8dd2-00aa004abd5e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:            HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[wmiprvse.exe]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[methodname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[interfaceid]
```

```
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclasspartitionid]
   Queries value:               HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{005ea477-f098-4d38-a3c2-efb77570be00}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{005ea477-f098-4d38-a3c2-efb77570be00}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{005ea477-f098-4d38-a3c2-efb77570be00}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{005ea477-f098-4d38-a3c2-efb77570be00}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{005ea477-f098-4d38-a3c2-efb77570be00}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[enabledebuggertracing]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[enableconsoletracing]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[enablefiletracing]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[consoletracingmask]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[filetracingmask]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[maxfilesize]
   Queries value:               HKLM\software\microsoft\tracing\tapi32[filedirectory]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{1639c72a-1a0a-47a4-921d-ee4a54fd909e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{1639c72a-1a0a-47a4-921d-ee4a54fd909e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{1639c72a-1a0a-47a4-921d-ee4a54fd909e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{1639c72a-1a0a-47a4-921d-ee4a54fd909e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{1639c72a-1a0a-47a4-921d-ee4a54fd909e}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{66df4d2a-d6c8-4cc8-98ce-d41df97bc4c0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{66df4d2a-d6c8-4cc8-98ce-d41df97bc4c0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{66df4d2a-d6c8-4cc8-98ce-d41df97bc4c0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{66df4d2a-d6c8-4cc8-98ce-d41df97bc4c0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{66df4d2a-d6c8-4cc8-98ce-d41df97bc4c0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{6cec9440-b380-4cb9-b34e-976dcb71c997}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{6cec9440-b380-4cb9-b34e-976dcb71c997}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:               HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{6cec9440-b380-4cb9-b34e-976dcb71c997}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
```

```
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{6cec9440-b380-4cb9-b34e-976dcb71c997}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{6cec9440-b380-4cb9-b34e-976dcb71c997}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{9242f92e-51ec-43bc-bc55-a2114102e8d0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{9242f92e-51ec-43bc-bc55-a2114102e8d0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{9242f92e-51ec-43bc-bc55-a2114102e8d0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[reader_sl.exe]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{9242f92e-51ec-43bc-bc55-a2114102e8d0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{9242f92e-51ec-43bc-bc55-a2114102e8d0}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{c46fb167-8b94-46b1-be86-be941a22332c}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{c46fb167-8b94-46b1-be86-be941a22332c}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{c46fb167-8b94-46b1-be86-be941a22332c}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:
HKLM\system\currentcontrolset\control\computername\computername[computername]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{c46fb167-8b94-46b1-be86-be941a22332c}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{c46fb167-8b94-46b1-be86-be941a22332c}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:
HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities[requestmakecall]
   Queries value:
HKU\.default\software\microsoft\windows\currentversion\telephony\handoffpriorities[requestmediacall]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[numproviders]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid0]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename0]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{df286e4f-26fb-4de8-88ec-f5ad9ebb2b76}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{df286e4f-26fb-4de8-88ec-f5ad9ebb2b76}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{df286e4f-26fb-4de8-88ec-f5ad9ebb2b76}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{df286e4f-26fb-4de8-88ec-f5ad9ebb2b76}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{df286e4f-26fb-4de8-88ec-f5ad9ebb2b76}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f18496b7-574d-425c-8b5e-f6f7bff87350}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberclsid]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f18496b7-574d-425c-8b5e-f6f7bff87350}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f18496b7-574d-425c-8b5e-f6f7bff87350}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[active]
   Queries value:              HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f18496b7-574d-425c-8b5e-f6f7bff87350}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[publisherid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f18496b7-574d-425c-8b5e-f6f7bff87350}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriptionid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriptionname]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[peruser]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[ownersid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[enabled]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[description]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[machinename]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[filtercriteria]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscribermoniker]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[eventclassapplicationid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberpartitionid]
   Queries value:            HKLM\software\microsoft\eventsystem\{26c409cc-ae86-11d1-b616-
00805fc79216}\subscriptions\{f98c5003-16f4-4e33-bca4-e92f4742ad27}-{00000000-0000-0000-0000-
000000000000}-{00000000-0000-0000-0000-000000000000}[subscriberapplicationid]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid1]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename1]
   Queries value:            HKLM\software\microsoft\tracing\kmddsp[enablefiletracing]
   Queries value:            HKLM\software\microsoft\tracing\kmddsp[filetracingmask]
   Queries value:            HKLM\software\microsoft\tracing\kmddsp[enableconsoletracing]
   Queries value:            HKLM\software\microsoft\tracing\kmddsp[consoletracingmask]
   Queries value:            HKLM\software\microsoft\tracing\kmddsp[maxfilesize]
   Queries value:            HKLM\software\microsoft\tracing\kmddsp[filedirectory]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid2]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename2]
   Queries value:            HKLM\software\microsoft\tracing\ndptsp[enablefiletracing]
   Queries value:            HKLM\software\microsoft\tracing\ndptsp[filetracingmask]
   Queries value:            HKLM\software\microsoft\tracing\ndptsp[enableconsoletracing]
   Queries value:            HKLM\software\microsoft\tracing\ndptsp[consoletracingmask]
   Queries value:            HKLM\software\microsoft\tracing\ndptsp[maxfilesize]
   Queries value:            HKLM\software\microsoft\tracing\ndptsp[filedirectory]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid3]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename3]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[enabledebuggertracing]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[consoletracingmask]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[enablefiletracing]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[filetracingmask]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[enableconsoletracing]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[maxfilesize]
   Queries value:            HKLM\software\microsoft\tracing\conftsp[filedirectory]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid4]
   Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename4]
   Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
   Queries value:            HKLM\software\microsoft\windows\currentversion\h323tsp[debuglevel]
   Queries value:            HKLM\software\microsoft\windows\currentversion\h323tsp[q931listenport]
   Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\h323tsp[q931alertingtimeout]
  Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gatewayaddress]
  Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gatewayenabled]
  Queries value:              HKLM\software\microsoft\windows\currentversion\h323tsp[h323proxyaddress]
  Queries value:              HKLM\software\microsoft\windows\currentversion\h323tsp[h323proxyenabled]
  Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gatekeeperenabled]
  Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gklogonphonenumberenabled]
  Queries value:
HKLM\software\microsoft\windows\currentversion\h323tsp[h323gklogonaccountnameenabled]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerid5]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony\providers[providerfilename5]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0000[netcfginstanceid]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0001[netcfginstanceid]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0002[netcfginstanceid]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0003[netcfginstanceid]
  Queries value:              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
  Queries value:              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[netcfginstanceid]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[netcfginstanceid]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[netcfginstanceid]
  Queries value:              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
  Queries value:              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
  Queries value:              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[wanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[enableforras]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[enableforrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[enableforoutboundrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[minwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[maxwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[driverdesc]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[fclientrole]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters[limitsimultaneousincomingcalls]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0006[calledidinformation]
  Queries value:              HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[wanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[enableforras]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[enableforrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[enableforoutboundrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[minwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[maxwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[driverdesc]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[fclientrole]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0005[calledidinformation]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[wanendpoints]
```

```
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[enableforras]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[enableforrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[enableforoutboundrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[minwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[maxwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[driverdesc]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[fclientrole]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0004[calledidinformation]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[netcfginstanceid]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[wanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[enableforras]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[enableforrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[enableforoutboundrouting]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[minwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[maxwanendpoints]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[driverdesc]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[fclientrole]
  Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e972-e325-11ce-bfc1-
08002be10318}\0007[calledidinformation]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\parameters[numberofrings]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters\quarantine[enabled]
  Queries value:              HKLM\software\microsoft\tracing\rasqec[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\rasqec[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\rasqec[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\rasqec[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\rasqec[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\rasqec[filedirectory]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\parameters\quarantine[autorefreshenabled]
  Queries value:              HKLM\software\microsoft\tracing\rasman[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\rasman[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\rasman[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\rasman[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\rasman[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\rasman[filedirectory]
  Queries value:              HKLM\software\microsoft\tracing\ppp[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\ppp[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\ppp[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\ppp[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\ppp[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\ppp[filedirectory]
  Queries value:              HKLM\software\microsoft\tracing\bap[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\bap[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\bap[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\bap[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\bap[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\bap[filedirectory]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[maxterminate]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[maxconfigure]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[maxfailure]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[maxreject]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[restarttimer]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[negotiatetime]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[defaultcallbackdelay]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[defaultportlimit]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[defaultsessiontimeout]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[defaultidletimeout]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[lowerbandwidththreshold]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[timebelowtheshold]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[baplistentimeout]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[unknownpackettracesize]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[echorequestinterval]
  Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp[idletimebeforeecho]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[missedechosbeforedisconnect]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp[dontnegotiatemultilinkonsinglelink]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp[parsedllpath]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[path]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateipcp]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatebacp]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatecbcp]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateccp]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateeap]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateipx]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatepap]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiateatcp]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[negotiatespap]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\chap[path]
  Queries value:            HKLM\software\microsoft\tracing\rasspap[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasspap[filetracingmask]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\perflib[disable
performance counters]
  Queries value:            HKLM\software\microsoft\tracing\rasspap[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasspap[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasspap[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasspap[filedirectory]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[jqs.exe]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[followstrictsequencing]
  Queries value:            HKLM\software\microsoft\tracing\raspap[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\raspap[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\raspap[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\raspap[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\raspap[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\raspap[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\raseap[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\raseap[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\raseap[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\raseap[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\raseap[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\raseap[filedirectory]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[path]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[path]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[path]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[path]
  Queries value:            HKLM\software\microsoft\tracing\rasccp[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasccp[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasccp[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasccp[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasccp[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasccp[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\rasbacp[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasbacp[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasbacp[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasbacp[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasbacp[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasbacp[filedirectory]
  Queries value:            HKLM\software\microsoft\tracing\rasiphlp[enablefiletracing]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[10]
  Queries value:            HKLM\software\microsoft\tracing\rasiphlp[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasiphlp[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasiphlp[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasiphlp[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasiphlp[filedirectory]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
  Queries value:
```

```
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[usedhcpaddressing]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[networkadapterguid]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[suppresswinsnameservers]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[suppressdnsnameservers]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[initialaddresspoolsize]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[allownetworkaccess]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[winsnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[winsnameserverbackup]
  Queries value:
HKLM\system\currentcontrolset\services\remoteaccess\parameters\ip[dnsnameservers]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\adapters\ndiswanip[ipconfig]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[dhcpipaddress]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[dhcpsubnetmask]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{4fe87b73-b12e-47d6-
82c4-fb0d4cf73262}[nameserverlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[dhcpipaddress]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[dhcpsubnetmask]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\netbt\parameters\interfaces\tcpip_{cac79791-bd6d-4f3e-
bcad-e3686652faee}[nameserverlist]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\controlprotocols\builtin[maxmsipcpoptioncfgcnt]
  Queries value:            HKLM\software\microsoft\tracing\rasipcp[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasipcp[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasipcp[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasipcp[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasipcp[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasipcp[filedirectory]
  Queries value:            HKLM\system\wpa\pnp[seed]
  Queries value:            HKLM\system\setup[osloaderpath]
  Queries value:            HKLM\system\setup[systempartition]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[loglevel]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[981f2d7e-b1f3-11d0-
8dd7-00c04fc3358c]
  Queries value:            HKLM\system\currentcontrolset\control\wmi\security[981f2d7d-b1f3-11d0-
8dd7-00c04fc3358c]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\jvm.dll[checkapphelp]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a00]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zone_elevation[explorer.exe]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[2101]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[unsecapp.exe]
  Queries value:            HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
  Queries value:            HKCU\software\microsoft\internet
explorer\ietld\lowmic[ietldllversionlow]
  Queries value:            HKCU\software\microsoft\internet
explorer\ietld\lowmic[ietldllversionhigh]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[{aeba21fa-782a-4a90-978d-b72164c80120}]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[privacyadvanced]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[alg.exe]
  Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[1h6wzb8f9vux2v7xspnwvurp]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings[warnonintranet]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1409]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1409]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1409]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1409]
  Sets/Creates value:       HKCU\software\microsoft\internet
explorer\phishingfilter[shownservicedownballoon]
  Sets/Creates value:       HKCU\software\microsoft\internet
explorer\recovery[clearbrowsinghistoryonexit]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1609]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1406]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1609]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[1406]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1609]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[1406]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1409]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\zones\3[1609]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1406]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1609]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[1406]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1[1406]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2[1406]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3[1406]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4[1406]
  Value changes:           HKCU\software\microsoft\internet explorer\phishingfilter[enabledv8]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Value changes:           HKCU\sessioninformation[programcount]
  Value changes:           HKLM\system\currentcontrolset\services\eventlog\application\microsoft
h.323 telephony service provider[eventmessagefile]
  Value changes:           HKLM\system\currentcontrolset\services\eventlog\application\microsoft
h.323 telephony service provider[typessupported]
  Value changes:           HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
```