Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	792
Risk Level:	10
Date Processed:	2016-05-18 10:38:46 (UTC)
Processing Time:	62.56 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe"

Sample ID:	3321
Type:	basic
Owner:	admin
Label:	543bd82ec71ae746e83c14eba28494df
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	147968 bytes
MD5:	543bd82ec71ae746e83c14eba28494df
SHA256:	b5835739dfcf21ab4869dea949ccc6038ea65be94f11307154e2c58a404b53ec
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
5	Abnormal sleep detected
4	Checks whether debugger is present
10	Creates malicious events: Clisbot [Worm]
7	Changes DNS name server
4	Terminates process under Windows subfolder
5	PE: Contains compressed section
5	Adds autostart object
5	Installs service

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe ["c:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe"]
Creates process:	C:\WINDOWS\regedit.exe [regedit.exe /s C:\DOCUME~1\Admin\LOCALS~1\Temp\rtf1.tmp]
Writes to process:	PID:308 C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe
Terminates process:	C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe
Terminates process:	C:\WINDOWS\regedit.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\1-4B4F4E4E494348492D5741-1
Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp
Creates:	C:\Documents and Settings\Admin\dlst.dat
Opens:	C:\WINDOWS\Prefetch\543BD82EC71AE746E83C14EBA2849-26981750.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\imm32.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:mylib\myfile
Opens:	C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe
Opens:	C:\WINDOWS\system32\apphelp.dll
Opens:	C:\WINDOWS\AppPatch\sysmain.sdb
Opens:	C:\WINDOWS\AppPatch\systest.sdb
Opens:	C:\WINDOWS\Temp
Opens:	C:\
Opens:	C:\WINDOWS
Opens:	C:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe.Manifest
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:dlst.dat
Opens:	C:\WINDOWS\Temp\58be9f66-5664-4dba-bd69-e7a34be8b0af
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp
Opens:	C:\WINDOWS\regedit.exe

Opens:	C:flh.dat
Opens:	C:pconfig
Opens:	C:dpconfig
Opens:	C:\WINDOWS\system32\mswsock.dll
Opens:	C:\WINDOWS\system32\hnetcfg.dll
Opens:	C:\WINDOWS\system32\wshtcpip.dll
Opens:	C:\WINDOWS\regedit.exe.Manifest
Opens:	C:\WINDOWS\regedit.exe.Config
Opens:	C:\WINDOWS\Prefetch\REGEDIT.EXE-1B606482.pf
Opens:	C:
Opens:	C:\WINDOWS\AppPatch
Opens:	C:\WINDOWS\Microsoft.NET
Opens:	C:\WINDOWS\Microsoft.NET\Framework
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v3.0
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Workflow Foundation
Opens:	C:\WINDOWS\system32
Opens:	C:\WINDOWS\WinSxS
Opens:	C:\WINDOWS\system32\ntdll.dll
Opens:	C:\WINDOWS\system32\kernel32.dll
Opens:	C:\WINDOWS\system32\unicode.nls
Opens:	C:\WINDOWS\system32\locale.nls
Opens:	C:\WINDOWS\system32\sorttbls.nls
Opens:	C:\WINDOWS\system32\msvcrt.dll
Opens:	C:\WINDOWS\system32\advapi32.dll
Opens:	C:\WINDOWS\system32\rpcrt4.dll
Opens:	C:\WINDOWS\system32\secur32.dll
Opens:	C:\WINDOWS\system32\gdi32.dll
Opens:	C:\WINDOWS\system32\user32.dll
Opens:	C:\WINDOWS\system32\shlwapi.dll
Opens:	C:\WINDOWS\system32\comdlg32.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\authz.dll
Opens:	C:\WINDOWS\system32\aclui.dll
Opens:	C:\WINDOWS\system32\ole32.dll
Opens:	C:\WINDOWS\system32\oleaut32.dll
Opens:	C:\WINDOWS\system32\ulib.dll
Opens:	C:\WINDOWS\system32\clb.dll
Opens:	C:\WINDOWS\system32\shimeng.dll
Opens:	C:\WINDOWS\AppPatch\AcGenral.dll
Opens:	C:\WINDOWS\system32\winmm.dll
Opens:	C:\WINDOWS\system32\msacm32.dll
Opens:	C:\WINDOWS\system32\version.dll
Opens:	C:\WINDOWS\system32\userenv.dll
Opens:	C:\WINDOWS\system32\uxtheme.dll
Opens:	C:\WINDOWS\system32\ctype.nls
Opens:	C:\WINDOWS\system32\sortkey.nls
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\MSIMTF.dll
Opens:	C:\WINDOWS\system32\narrhook.dll
Opens:	C:\WINDOWS\system32\oleacc.dll
Opens:	C:\WINDOWS\system32\msvcp60.dll
Opens:	C:\WINDOWS\system32\oleaccrc.dll
Opens:	C:\WINDOWS\system32\win32k.sys
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v3.0\Windows Workflow Foundation\PerfCounters.reg
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\system32\ACLUI.dll.123.Manifest
Opens:	C:\WINDOWS\system32\ACLUI.dll.123.Config
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp
Writes to:	C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp
Writes to:	C:\Documents and Settings\Admin\dlst.dat
Reads from:	C:\WINDOWS\Temp\543bd82ec71ae746e83c14eba28494df.exe
Reads from:	C:\WINDOWS\Prefetch\REGEDIT.EXE-1B606482.pf
Reads from:	C:\Documents and Settings\Admin\Local Settings\Temp\rtf1.tmp

Network Events

Connects to:	31.193.4.140:9091
Connects to:	255.255.255.255:9091

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\software\microsoft\microsoft windows nt 4.0
Creates key:	HKCU\software\microsoft\multimedia\audio
Creates key:	HKCU\software\microsoft\multimedia\audio compression manager\
Creates key:	HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key:	HKCU\software\microsoft\multimedia\audio compression manager\priority v4.00
Creates key:	HKCU\software\microsoft\windows\currentversion\run
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\543bd82ec71ae746e83c14eba28494df.exe

```
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  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\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\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  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:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  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\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  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\windows nt\currentversion\image file execution
options\oleaut32.dll
  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 nt\currentversion\image file execution
options\wininet.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\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  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:                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\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  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\543bd82ec71ae746e83c14eba28494df.exe
  Opens key:                HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
```

```
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  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\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:                HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\543bd82ec71ae746e83c14eba28494df.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\software\sophos
  Opens key:                HKLM\software\g data
  Opens key:                HKLM\software\doctor web
  Opens key:                HKLM\software\kasperskylab
  Opens key:                HKLM\software\eset
  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\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}
  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\appcompatflags\custom\regedit.exe
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  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\regedit.exe
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\authz.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\aclui.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ulib.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clb.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:               HKLM\system\setup
  Opens key:               HKLM\system\currentcontrolset\control\nls\locale
  Opens key:               HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:               HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:               HKLM\software\microsoft\audiocompressionmanager\drivercache
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
  Opens key:               HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
  Opens key:               HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
  Opens key:               HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
  Opens key:               HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
  Opens key:               HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
  Opens key:               HKLM\system\currentcontrolset\control\mediaresources\acm
  Opens key:               HKLM\system\currentcontrolset\control\productoptions
  Opens key:               HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:               HKLM\software\policies\microsoft\windows\system
  Opens key:               HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:               HKCU\software\microsoft\windows\currentversion\policies\system
  Queries value:           HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:           HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:           HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\compatibility32[543bd82ec71ae746e83c14eba28494df]
  Queries value:           HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[543bd82ec71ae746e83c14eba28494df]
```

```
  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[multiuilanguageid]
  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[543bd82ec71ae746e83c14eba28494df.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\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
  Queries value:              HKLM\system\wpa\mediacenter[installed]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:              HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
   Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
   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:          HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:          HKLM\software\microsoft\microsoft windows nt 4.0[oid]
  Queries value:          HKLM\software\microsoft\microsoft windows nt 4.0[gid]
  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}[dhcpnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4fe87b73-b12e-47d6-82c4-
fb0d4cf73262}[dhcpnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{cac79791-bd6d-4f3e-bcad-
e3686652faee}[dhcpnameserver]
  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\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[regedit]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[regedit]
  Queries value:          HKLM\system\setup[systemsetupinprogress]
  Queries value:          HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:          HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:             HKCU\software\microsoft\multimedia\audio[systemformats]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
  Queries value:
```

```
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
  Queries value:            HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
  Queries value:            HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:            HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:            HKCU\control panel\desktop[lamebuttontext]
  Sets/Creates value:       HKLM\software\microsoft\microsoft windows nt 4.0[guid]
  Sets/Creates value:       HKCU\software\microsoft\windows\currentversion\run[dskchk]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
  Value changes:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
```