Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	19
Risk Level:	6
Date Processed:	2016-04-08 09:39:50 (UTC)
Processing Time:	60.0 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ToggleService32.exe"
Sample ID:	6
Type:	basic
Owner:	admin
Label:	ToggleService32.exe
Date Added:	2016-04-08 09:39:50 (UTC)
File Type:	PE32:win32
File Size:	10254 bytes
MD5:	1439e0552127dda0c66b7be1eadb723d
SHA256:	89e815c8779e61dda1e5f6aa0af737361ffc6296c25300e82a5c23dcc165f82a
Description:	None

Pattern Matching Results

6 Writes to system32 folder
2 PE: Nonstandard section
6 PE: File has TLS callbacks
3 Writes to a log file [Info]
4 Terminates process under Windows subfolder
3 Long sleep detected

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\ToggleService32.exe ["c:\windows\temp\ToggleService32.exe"]
Creates process:	C:\WINDOWS\system32\msdtc.exe [C:\WINDOWS\system32\msdtc.exe]
Creates process:	C:\WINDOWS\system32\svchost.exe [C:\WINDOWS\System32\svchost.exe -k eapsvcs]
Loads service:	Alerter [C:\WINDOWS\system32\svchost.exe -k LocalService]
Loads service:	ALG [C:\WINDOWS\System32\alg.exe]
Loads service:	AppMgmt [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Loads service:	BITS [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Loads service:	Browser [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Loads service:	TrkWks [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Loads service:	MSDTC [C:\WINDOWS\system32\msdtc.exe]
Loads service:	DNSCache [C:\WINDOWS\system32\svchost.exe -k NetworkService]
Loads service:	EAPHost [C:\WINDOWS\System32\svchost.exe -k eapsvcs]
Loads service:	CISVC [C:\WINDOWS\system32\cisvc.exe]
Terminates process:	C:\WINDOWS\system32\svchost.exe
Creates remote thread:	System

Named Object Events

Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates event:	\BaseNamedObjects\EVENT_MSDTC_STARTING
Creates event:	\BaseNamedObjects\DINPUTWINMM
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates event:	\BaseNamedObjects\crypt32LogoffEvent
Creates event:	\BaseNamedObjects\MSDTC_NAMED_EVENT
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\Documents and Settings\Admin\output.txt
Creates:	C:\WINDOWS\system32\MsDtc\Trace\dtctrace.log
Opens:	C:\WINDOWS\Prefetch\TOGGLESERVICE32.EXE-310AE5F8.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\Documents and Settings\Admin\output.txt
Opens:	C:\WINDOWS\Prefetch\MSDTC.EXE-0E6E4AF7.pf
Opens:	C:\WINDOWS\system32
Opens:	C:\WINDOWS\system32\msdtctm.dll
Opens:	C:\WINDOWS\system32\dnsapi.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\msdtclog.dll
Opens:	C:\WINDOWS\system32\msdtcprx.dll
Opens:	C:\WINDOWS\system32\msvcp60.dll

```
  Opens:                  C:\WINDOWS\system32\mtxclu.dll
  Opens:                  C:\WINDOWS\system32\comres.dll
  Opens:                  C:\WINDOWS\system32\wsock32.dll
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\WINDOWS\system32\mswsock.dll
  Opens:                  C:\WINDOWS\system32\xolehlp.dll
  Opens:                  C:\WINDOWS\system32\shimeng.dll
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:                  C:\WINDOWS\system32\msacm32.dll
  Opens:                  C:\WINDOWS\system32\uxtheme.dll
  Opens:                  C:\WINDOWS\system32\imm32.dll
  Opens:                  C:\WINDOWS\system32\clusapi.dll
  Opens:                  C:\WINDOWS\system32\resutils.dll
  Opens:                  C:\WINDOWS\system32\rpcss.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\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\comctl32.dll
  Opens:                  C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\comctl32.dll.124.Config
  Opens:                  C:\WINDOWS\system32\mtxoci.dll
  Opens:                  C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
  Opens:                  C:\WINDOWS\system32\ntmarta.dll
  Opens:                  C:\WINDOWS\system32\samlib.dll
  Opens:                  C:\WINDOWS\system32\winlogon.exe
  Opens:                  C:\WINDOWS\system32\xpsp2res.dll
  Opens:                  C:\WINDOWS\system32\eapsvc.dll
  Opens:                  C:\WINDOWS\system32\eapphost.dll
  Opens:                  C:\WINDOWS\system32\MSDtc\trace\dtctrace.log
  Opens:                  C:\WINDOWS\system32\crypt32.dll
  Opens:                  C:\WINDOWS\system32\MsDtc\Trace
  Opens:                  C:\WINDOWS\system32\msasn1.dll
  Opens:                  C:\WINDOWS\system32\rastls.dll
  Opens:                  C:\WINDOWS\system32\raschap.dll
  Opens:                  C:\WINDOWS\system32\clbcatq.dll
  Opens:                  C:\WINDOWS\system32\MsDtc\Trace\dtctrace.log
  Opens:                  C:\WINDOWS\Registration\R000000000007.clb
  Opens:                  C:\WINDOWS\system32\MsDtc
  Opens:                  C:\WINDOWS\system32\MsDtc\MSDTC.LOG
  Opens:                  C:\WINDOWS\System32\drivers\etc\lmhosts
  Opens:                  C:\WINDOWS\system32\drivers\ipnat.sys
  Writes to:              C:\Documents and Settings\Admin\output.txt
  Writes to:              C:\WINDOWS\system32\MsDtc\Trace\dtctrace.log
  Writes to:              C:\WINDOWS\system32\MsDtc\MSDTC.LOG
  Reads from:             C:\Documents and Settings\Admin\output.txt
  Reads from:             C:\WINDOWS\system32\MsDtc\Trace\dtctrace.log
  Reads from:             C:\WINDOWS\Registration\R000000000007.clb
```

Windows Registry Events

```
  Creates key:            HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Creates key:            HKLM\system
  Creates key:            HKLM\system\currentcontrolset
  Creates key:            HKLM\system\currentcontrolset\control
  Creates key:            HKLM\system\currentcontrolset\control\mediaproperties
  Creates key:            HKLM\system\currentcontrolset\control\mediaproperties\privateproperties
  Creates key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick
  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:            HKU\.default\software\microsoft\multimedia\audio
  Creates key:            HKU\.default\software\microsoft\multimedia\audio compression manager\
  Creates key:            HKU\.default\software\microsoft\multimedia\audio compression
manager\msacm
  Creates key:            HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00
  Creates key:            HKLM\software\microsoft\windows nt\currentversion\tracing
  Creates key:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc
```

```
  Creates key:              HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc\traceidentifier
  Creates key:              HKLM\system\currentcontrolset\services\eaphost\parameters
  Creates key:              HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost
  Creates key:              HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost\traceidentifier
  Creates key:              HKLM\system\currentcontrolset\services\rasman\ppp\eap
  Creates key:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\13
  Creates key:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\25
  Creates key:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26
  Creates key:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4
  Creates key:              HKLM\software\classes
  Creates key:              HKLM\system\currentcontrolset\enum\root\legacy_ipnat\0000\control
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\toggleservice32.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\msvcrt.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\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\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\toggleservice32.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msdtc.exe
  Opens key:                HKLM\system\wpa\tabletpc
  Opens key:                HKLM\system\wpa\mediacenter
  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\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\dnsapi.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\gdi32.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\msdtclog.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  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\wsock32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mtxclu.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msdtcprx.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\mswsock.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\xolehlp.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msdtctm.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\oleaut32.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\shlwapi.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\userenv.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.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\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  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\clusapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\resutils.dll
  Opens key:                HKLM\software\microsoft\msdtc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc
  Opens key:                HKLM\software\microsoft\xaincptr\two_pipe_trace
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  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\software\microsoft\windows\currentversion\explorer\performance
  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\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\control panel\international
  Opens key:                HKLM\system\currentcontrolset\control\servicecurrent
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msdtc.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\classes
  Opens key:                HKCR\cid
  Opens key:                HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9
  Opens key:                HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\description
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\svcid
  Opens key:                 HKCR\svcid
  Opens key:                 HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\host
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\clsid
  Opens key:                 HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\protocol
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\endpoint
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties\log
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties\log\size
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mtxoci.dll
  Opens key:                 HKLM\software\microsoft\msdtc\mtxoci
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\cluster server
  Opens key:                 HKLM\software\microsoft\msdtc\security
  Opens key:                 HKLM\system\currentcontrolset\control\asr
  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\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe
  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:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c
  Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\description
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\description
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\svcid
  Opens key:                 HKCR\svcid\6407e780-7e5d-11d0-8ce6-00c04fdc877e
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\host
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\clsid
  Opens key:                 HKCR\svcid\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\protocol
  Opens key:                 HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\endpoint
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\description
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\svcid
  Opens key:                 HKCR\svcid\01366d42-c04e-11d1-b1c0-00c04fc2f3ef
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\host
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\clsid
  Opens key:                 HKCR\svcid\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\protocol
  Opens key:                 HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\endpoint
  Opens key:                 HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties\log\path
  Opens key:                 HKU\.default\software\policies\microsoft\control panel\desktop
  Opens key:                 HKU\.default\control panel\desktop
  Opens key:                 HKU\.default\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                 HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
  Opens key:                 HKU\.default\software\microsoft\windows\currentversion\thememanager
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\svchost
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\svchost\eapsvcs
  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\wldap32.dll
  Opens key:                 HKLM\system\currentcontrolset\services\ldap
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntmarta.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\svchost.exe\rpcthreadpoolthrottle
  Opens key:                 HKLM\system\currentcontrolset\control\lsa
  Opens key:                 HKLM\system\currentcontrolset\services
  Opens key:                 HKLM\system\currentcontrolset\services\eaphost
  Opens key:                 HKLM\system\currentcontrolset\services\eaphost\parameters
  Opens key:                 HKLM\software\microsoft\rpc\securityservice
  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\eapsvc.dll
  Opens key:                 HKLM\system\currentcontrolset\control\wmi\security
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions
  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\services\crypt32\performance
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\eapphost.dll
  Opens key:                 HKLM\hardware\description\system\centralprocessor\0
  Opens key:                 HKLM\system\currentcontrolset\services\eaphost\methods
  Opens key:                 HKLM\software\microsoft\com3
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:                 HKLM\software\microsoft\com3\debug
  Opens key:                 HKCU\software\classes\
  Opens key:                 HKU\
  Opens key:                 HKCR\clsid
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\treatas
  Opens key:                 HKCR\
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\inprocserver32
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\inprocserverx86
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\localserver32
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\inprochandler32
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\inprochandlerx86
  Opens key:                 HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\localserver
  Opens key:                 HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\treatas
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprocserver32
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprocserverx86
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\localserver32
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprochandler32
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprochandlerx86
  Opens key:                 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\localserver
  Opens key:                 HKCR\appid\{8c482dce-2644-4419-aeff-189219f916b9}
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed
  Opens key:                 HKCR\interface\{7ed70824-03ad-41c1-ab1a-950621776881}
  Opens key:                 HKCR\interface\{7ed70824-03ad-41c1-ab1a-950621776881}\proxystubclsid32
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\treatas
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprocserver32
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprocserverx86
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\localserver32
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprochandler32
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprochandlerx86
  Opens key:                 HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\localserver
```

```
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\svcid
   Opens key:                 HKCR\svcid\ced2de40-bff6-11ce-9de8-00aa00a3f464
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\host
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\clsid
   Opens key:                 HKCR\svcid\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\protocol
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\endpoint
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\customproperties
   Opens key:                 HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\customproperties\dac
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\treatas
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\treatas
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserver32
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserverx86
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprocserverx86
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\localserver32
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\localserver32
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprochandler32
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprochandlerx86
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprochandlerx86
   Opens key:                 HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\localserver
   Opens key:                 HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\localserver
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\treatas
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\treatas
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprocserverx86
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\localserver32
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\localserver32
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprochandler32
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86
   Opens key:                 HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\localserver
   Opens key:                 HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\localserver
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\treatas
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\treatas
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprocserverx86
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\localserver32
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\localserver32
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprochandler32
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86
   Opens key:                 HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\localserver
   Opens key:                 HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\localserver
   Opens key:                 HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}
   Opens key:                 HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}
   Opens key:                 HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\treatas
   Opens key:                 HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\treatas
```

```
  Opens key:                  HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32
  Opens key:                  HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\inprocserverx86
  Opens key:                  HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
  Opens key:                  HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\localserver32
  Opens key:                  HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\localserver32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\inprochandler32
  Opens key:                  HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
  Opens key:                  HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86
  Opens key:                  HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\localserver
  Opens key:                  HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\localserver
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\treatas
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\treatas
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\inprocserverx86
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\localserver32
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\localserver32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\inprochandler32
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86
  Opens key:                  HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\localserver
  Opens key:                  HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\localserver
  Opens key:                  HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\treatas
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\treatas
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprocserver32
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprocserverx86
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprocserverx86
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\localserver32
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\localserver32
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprochandler32
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprochandlerx86
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprochandlerx86
  Opens key:                  HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\localserver
  Opens key:                  HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\localserver
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                  HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\treatas
  Opens key:                  HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\treatas
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32
  Opens key:                  HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\inprocserverx86
  Opens key:                  HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\localserver32
  Opens key:                  HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\localserver32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\inprochandler32
  Opens key:                  HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
  Opens key:                HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\localserver
  Opens key:                HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\localserver
  Opens key:                HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\treatas
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\treatas
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprocserver32
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprocserverx86
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\localserver32
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver32
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprochandler32
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprochandlerx86
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\localserver
  Opens key:                HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver
  Opens key:                HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-00a0c9083365}
  Opens key:                HKLM\system\currentcontrolset\services\ipnat
  Opens key:                HKLM\system\currentcontrolset\services\ipnat\enum
  Opens key:                HKLM\system\currentcontrolset\enum
  Opens key:                HKLM\system\currentcontrolset\enum\root\legacy_ipnat\0000
  Opens key:                HKLM\system\currentcontrolset\hardware profiles\current
  Opens key:                HKLM\system\currentcontrolset\hardware profiles\0001
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\enum
  Opens key:                HKLM\system\currentcontrolset\hardware
profiles\0001\system\currentcontrolset\enum\root\legacy_ipnat\0000
  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\software\microsoft\rpc[maxrpcsize]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\system\wpa\mediacenter[installed]
  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:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  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:
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:
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\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\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\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
   Queries value:            HKLM\system\setup[systemsetupinprogress]
   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\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
   Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[msdtc]
   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:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:            HKLM\software\microsoft\msdtc[dtcenablelrm]
   Queries value:            HKLM\software\microsoft\msdtc[rpcqoscapabilities]
   Queries value:            HKLM\software\microsoft\msdtc[rpcqosidentity]
   Queries value:            HKLM\software\microsoft\msdtc[rpcauthnsvc]
   Queries value:            HKLM\software\microsoft\msdtc[rpcauthnlevel]
   Queries value:            HKLM\software\microsoft\msdtc[tracecmerr]
```

```
  Queries value:            HKLM\software\microsoft\msdtc[numcccimhistoryentries]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\misc[debugtracinglevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\misc[disabletracing]
  Queries value:            HKLM\software\microsoft\msdtc[dtcmemalloc]
  Queries value:            HKLM\software\microsoft\msdtc[membuffersize]
  Queries value:            HKLM\software\microsoft\msdtc[cmcancelrpcafter]
  Queries value:            HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
  Queries value:            HKLM\software\microsoft\msdtc[cmmaxidlepings]
  Queries value:            HKLM\software\microsoft\msdtc[cmpingfreqsecs]
  Queries value:            HKLM\software\microsoft\msdtc[cmverbose]
  Queries value:            HKLM\software\microsoft\msdtc[donotgoidle]
  Queries value:            HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
  Queries value:            HKLM\software\microsoft\msdtc[disablesinglephase]
  Queries value:            HKLM\software\microsoft\msdtc[usetiponly]
  Queries value:            HKLM\software\microsoft\msdtc[createresourcemanagertimeout]
  Queries value:            HKLM\software\microsoft\msdtc[overridetiphostname]
  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\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:            HKLM\software\microsoft\msdtc[turnoffbadmsgevents]
  Queries value:            HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]
  Queries value:            HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]
  Queries value:            HKLM\software\microsoft\msdtc[tcpnodelay]
  Queries value:            HKLM\software\microsoft\msdtc[dtcmaxsessions]
  Queries value:            HKLM\software\microsoft\msdtc[disabletippassthrucheck]
  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:          HKCU\control panel\desktop[smoothscroll]
  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]
  Queries value:          HKCU\control panel\international[locale]
  Queries value:          HKLM\system\currentcontrolset\control\servicecurrent[]
  Queries value:          HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\description[]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\svcid[]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\host[]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\clsid[]
  Queries value:          HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\protocol[]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\endpoint[]
  Queries value:          HKCR\cid\2460f484-6eb1-4d02-91b6-
690602ba23f9\customproperties\log\size[]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[oraclexalib]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[oracleocilib]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[enabletrace]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath]
  Queries value:          HKLM\software\microsoft\msdtc\mtxoci[debugtrace]
  Queries value:          HKLM\software\microsoft\msdtc\security[accountname]
  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\software\microsoft\windows
nt\currentversion\compatibility32[svchost]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[svchost]
  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\msdtc\security[domaincontrollerstate]
  Queries value:              HKLM\software\microsoft\msdtc\security[networkdtcaccess]
  Queries value:              HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
  Queries value:              HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
  Queries value:              HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
  Queries value:              HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
  Queries value:              HKLM\software\microsoft\msdtc\security[xatransactions]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:              HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\description[]
  Queries value:              HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\description[]
  Queries value:              HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\svcid[]
  Queries value:              HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\host[]
  Queries value:              HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\clsid[]
  Queries value:              HKCR\svcid\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
  Queries value:              HKU\.default\software\microsoft\multimedia\audio[systemformats]
  Queries value:              HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\protocol[]
  Queries value:              HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\endpoint[]
  Queries value:              HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\description[]
  Queries value:              HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\svcid[]
  Queries value:              HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\host[]
  Queries value:              HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\clsid[]
  Queries value:              HKCR\svcid\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider[]
  Queries value:              HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\protocol[]
  Queries value:              HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\endpoint[]
  Queries value:              HKCR\cid\2460f484-6eb1-4d02-91b6-
690602ba23f9\customproperties\log\path[]
  Queries value:              HKU\.default\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
  Queries value:              HKU\.default\control panel\desktop[multiuilanguageid]
  Queries value:              HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
  Queries value:              HKU\.default\control panel\desktop[smoothscroll]
  Queries value:              HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[personal]
  Queries value:              HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local settings]
  Queries value:
HKU\.default\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:              HKU\.default\control panel\desktop[lamebuttontext]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\svchost[eapsvcs]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\svchost\eapsvcs[coinitializesecurityparam]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\svchost\eapsvcs[authenticationlevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\svchost\eapsvcs[impersonationlevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\svchost\eapsvcs[authenticationcapabilities]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\svchost\eapsvcs[defaultrpcstacksize]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:            HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:            HKLM\system\currentcontrolset\services\eaphost\parameters[servicedll]
  Queries value:            HKLM\system\currentcontrolset\services\eaphost\parameters[servicemain]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[9]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  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\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\services\eaphost\parameters[waithint]
  Queries value:            HKLM\system\currentcontrolset\services\eaphost\parameters[peerinstalled]
  Queries value:
HKLM\system\currentcontrolset\services\eaphost\parameters[authenticatorinstalled]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[requestsessionup]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxbuffers]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\loggingoptions[maxfilesize]
  Queries value:            HKLM\hardware\description\system\centralprocessor\0[~mhz]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[friendlyname]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[properties]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[configuipath]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[standalonesupported]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[mppeencryptionsupported]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[treatasmsmethod]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[path]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[friendlyname]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[properties]
  Queries value:            HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[configuipath]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[standalonesupported]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[mppeencryptionsupported]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[treatasmsmethod]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[path]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[friendlyname]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[properties]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[configuipath]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[standalonesupported]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[mppeencryptionsupported]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[treatasmsmethod]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[path]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[friendlyname]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[properties]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[configuipath]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[standalonesupported]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[mppeencryptionsupported]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[treatasmsmethod]
   Queries value:              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[path]
   Queries value:              HKLM\software\microsoft\com3[com+enabled]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[68fdd900-4a3e-11d1-
84f4-0000f80464e3]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[ec1427e2-51be-4ffa-
a22d-a876261e580d]
   Queries value:              HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
   Queries value:              HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
   Queries value:              HKLM\software\microsoft\com3[regdbversion]
   Queries value:              HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[appid]
   Queries value:              HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[dllsurrogate]
   Queries value:              HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[localservice]
   Queries value:              HKLM\system\currentcontrolset\control\wmi\security[1b1d4ff4-f27b-4c99-
8bd7-da8f1a74051a]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[uniqueid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[active]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[level]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules[controlflags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[uniqueid]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
   Queries value:              HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}[appid]
   Queries value:              HKCR\appid\{8c482dce-2644-4419-aeff-189219f916b9}[dllsurrogate]
   Queries value:              HKCR\appid\{8c482dce-2644-4419-aeff-189219f916b9}[localservice]
   Queries value:              HKCR\interface\{7ed70824-03ad-41c1-ab1a-950621776881}\proxystubclsid32[]
   Queries value:              HKCR\clsid\{1510fb87-5676-40b9-a227-
5d0b66866f81}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprocserver32[]
   Queries value:              HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}[appid]
   Queries value:              HKCR\clsid\{1510fb87-5676-40b9-a227-
5d0b66866f81}\inprocserver32[threadingmodel]
   Queries value:              HKLM\software\microsoft\msdtc[servicenetworkprotocols]
   Queries value:              HKLM\software\microsoft\msdtc[notracking]
   Queries value:              HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\svcid[]
   Queries value:              HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\host[]
   Queries value:              HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\clsid[]
   Queries value:              HKCR\svcid\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider[]
   Queries value:              HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\protocol[]
   Queries value:              HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\endpoint[]
   Queries value:              HKCR\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprocserver32[]
   Queries value:              HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}[appid]
   Queries value:              HKCR\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserver32[threadingmodel]
   Queries value:              HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
   Queries value:              HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}[appid]
   Queries value:              HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[threadingmodel]
   Queries value:              HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
```

```
  Queries value:               HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}[appid]
  Queries value:               HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[threadingmodel]
  Queries value:               HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
  Queries value:               HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}[appid]
  Queries value:               HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[threadingmodel]
  Queries value:               HKLM\software\microsoft\msdtc[transactionbridge]
  Queries value:               HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
  Queries value:               HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}[appid]
  Queries value:               HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[threadingmodel]
  Queries value:               HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisabletypelib]
  Queries value:               HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisableall]
  Queries value:               HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperuser]
  Queries value:               HKCR\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprocserver32[]
  Queries value:               HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}[appid]
  Queries value:               HKCR\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprocserver32[threadingmodel]
  Queries value:               HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
  Queries value:               HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}[appid]
  Queries value:               HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[threadingmodel]
  Queries value:               HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisabletypelib]
  Queries value:               HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisableall]
  Queries value:               HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperuser]
  Queries value:               HKCR\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserver32[]
  Queries value:               HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}[appid]
  Queries value:               HKCR\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprocserver32[threadingmodel]
  Queries value:               HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisabletypelib]
  Queries value:               HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisableall]
  Queries value:               HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperuser]
  Queries value:               HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisabletypelib]
  Queries value:               HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisableall]
  Queries value:               HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperuser]
  Queries value:               HKLM\system\currentcontrolset\services\ipnat[imagepath]
  Queries value:               HKLM\system\currentcontrolset\services\ipnat[objectname]
  Queries value:               HKLM\system\currentcontrolset\services\ipnat[type]
  Queries value:               HKLM\system\currentcontrolset\services\ipnat\enum[count]
  Queries value:               HKLM\system\currentcontrolset\services\ipnat\enum[0]
  Queries value:               HKLM\system\currentcontrolset\enum\root\legacy_ipnat\0000[configflags]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc[logsessionname]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc[active]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc[controlflags]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc\traceidentifier[guid]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapsvc\traceidentifier[bitnames]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost[logsessionname]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost[active]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost[controlflags]
  Sets/Creates value:          HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost\traceidentifier[guid]
  Sets/Creates value:          HKLM\software\microsoft\windows
```

```
nt\currentversion\tracing\microsoft\eapphost\traceidentifier[bitnames]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:
HKLM\system\currentcontrolset\enum\root\legacy_ipnat\0000\control[activeservice]
```