Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 6, Task ID: 19

Task ID: 19 Risk Level:

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: Type: basic Owner: admin

Label: ToggleService32.exe 2016-04-08 09:39:50 (UTC) Date Added:

PE32:win32 File Type: File Size: 10254 bytes

1439e0552127dda0c66b7be1eadb723d MD5:

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]

Terminates process under Windows subfolder

3 Long sleep detected

Static Events

Anomaly: PE: Contains a virtual section

PE: Contains one or more non-standard sections Anomaly:

Anomaly: PE: File contain TLS callbacks

Process/Thread Events

C:\WINDOWS\Temp\ToggleService32.exe Creates process:

["c:\windows\temp\ToggleService32.exe"]

C:\WINDOWS\system32\msdtc.exe [C:\WINDOWS\system32\msdtc.exe] Creates process: Creates process:

eapsvcs]

Alerter [C:\WINDOWS\system32\svchost.exe -k LocalService] Loads service:

Loads service: ALG [C:\WINDOWS\System32\alg.exe]

AppMgmt [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service: Loads service: BITS [C:\WINDOWS\system32\svchost.exe -k netsvcs] Browser [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service: TrkWks [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service:

Loads service: MSDTC [C:\WINDOWS\system32\msdtc.exe]

Loads service: DNSCache [C:\WINDOWS\system32\svchost.exe -k NetworkService]

EAPHost [C:\WINDOWS\System32\svchost.exe -k eapsvcs] Loads service:

Loads service: CISVC [C:\WINDOWS\system32\cisvc.exe] Terminates process:

C:\WINDOWS\system32\svchost.exe

Creates remote thread: System

Named Object Events

\BaseNamedObjects\SHIMLIB_LOG_MUTEX Creates mutex: \BaseNamedObjects\EVENT_MSDTC_STARTING Creates event:

Creates event: \BaseNamedObjects\DINPUTWINMM

Creates event: \BaseNamedObjects\userenv: User Profile setup event

Creates event: \BaseNamedObjects\crypt32LogoffEvent \BaseNamedObjects\MSDTC_NAMED_EVENT Creates 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 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: Opens: C:\WINDOWS\system32\ws2help.dll C:\WINDOWS\system32\msdtclog.dll Opens: C:\WINDOWS\system32\msdtcprx.dll Opens: Opens: C:\WINDOWS\system32\msvcp60.dl1

C:\WINDOWS\system32\mtxclu.dll Opens: 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 C:\WINDOWS\system32\shimeng.dll Opens: C:\WINDOWS\AppPatch\sysmain.sdb Opens: Opens: C:\WINDOWS\AppPatch\systest.sdb C:\WINDOWS\AppPatch\AcGenral.dll Opens: 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 Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Opens:

C:\WINDOWS\system32\SHELL32.dll.124.Config Opens: Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll

Opens: C:\WINDOWS\WindowsShell.Manifest C:\WINDOWS\WindowsShell.Config Opens: Opens: C:\WINDOWS\system32\comctl32.dll

Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest C:\WINDOWS\system32\comctl32.dll.124.Config Opens:

Opens: C:\WINDOWS\system32\mtxoci.dll

Opens: C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf

C:\WINDOWS\system32\ntmarta.dll Opens: 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 C:\WINDOWS\system32\clbcatq.dll Opens:

Opens: C:\WINDOWS\system32\MsDtc\Trace\dtctrace.log Opens: C:\WINDOWS\Registration\R00000000007.clb

Opens: C:\WINDOWS\system32\MsDtc

Opens: C:\WINDOWS\system32\MsDtc\MSDTC.LOG Opens: C:\WINDOWS\Svstem32\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\R00000000007.clb

Windows Registry Events

Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters

Creates key:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm

Creates kev: HKLM\svstem

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:

Creates key: HKCU\software\microsoft\multimedia\audio

Creates key: HKCU\software\microsoft\multimedia\audio compression manager\ Creates key: $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc multimedia\audio compression manager\mbox{\sc manager}} \mbox{\sc manager\mbox{\sc manager\mbox{\sc manager}}} \mbox{\sc manager\mbox{\sc manager\mbox{\sc manager\mbox{\sc manager}}} \mbox{\sc manager\mbox{\sc m$ Creates key: HKCU\software\microsoft\multimedia\audio compression manager\priority

v4.00

Creates kev: 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 kev: HKLM\software\microsoft\windows nt\currentversion\tracing\microsoft\eapsvc\traceidentifier

 ${\tt HKLM \backslash system \backslash current control set \backslash services \backslash eaphost \backslash parameters}$ Creates key:

Creates key: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\tracing\microsoft\eapphost|\\$

Creates key: HKLM\software\microsoft\windows nt\currentversion\tracing\microsoft\eapphost\traceidentifier

HKLM\system\currentcontrolset\services\rasman\ppp\eap Creates key: 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

 $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ enum \+ root \+ legacy_ipnat \+ 0000 \+ control$ Creates key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\toggleservice32.exe

HKIM\system\currentcontrolset\control\terminal server Opens kev:

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\secur32.dll

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

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\software\microsoft\windows nt\currentversion\diagnostics Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msvcrt.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev:

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 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \policies \microsoft \windows \safer \code identifiers \end{tabular}$ Opens key:

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

 $\label{lem:hklmsoftware} \mbox{ HKLM\software\mbox{\sc microsoft\windows nt\currentversion\sc file execution} \\$ Opens key:

options\toggleservice32.exe\rpcthreadpoolthrottle

HKLM\software\policies\microsoft\windows nt\rpc Opens kev: 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

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key:

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: options\msdtclog.dll

 $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens key:

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: options\netapi32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution

HKLM\software\microsoft\windows nt\currentversion\image file execution

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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\shimeng.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 HKLM\system\setup Opens key: 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: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility $\label{lem:hklm} \mbox{HKLM\software\mbox{\sc microsoft\windows}} \ \ \mbox{nt\current\version\windows}$ Opens key: Opens key: HKLM\software\microsoft\ole Opens key: HKCR\interface HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: Opens key: HKLM\system\currentcontrolset\control\computername Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 HKLM\software\microsoft\xaincptr\two_pipe_trace Opens key: Opens key: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32$ Opens key: Opens key: HKLM\software\microsoft\oleaut Opens key: HKLM\software\microsoft\oleaut\userera Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache$ Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.im aadpcm$ Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msadpcm$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711 Opens key: Opens key: Opens kev: Opens key: Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1 Opens key: $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. sl_anet$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2 $\label{thm:local} \verb+HKLM\software\microsoft\audiocompression manager\driver cache\mbox{\sc m.} 13 acm$ Opens key: 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: $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced$ HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: ${\it HKLM} \verb|\system| current controlset| control| product options$ Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders HKLM\software\policies\microsoft\windows\system Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\thememanager HKCU\control panel\international Opens key: Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msdtc.exe\rpcthreadpoolthrottle HKLM\software\classes Opens key: Opens key: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9 Opens key: Opens key: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\description

```
HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\svcid
  Opens key:
  Opens key:
                                  HKCR\svcid
                                  HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464
  Opens kev:
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\host
  Opens key:
  Opens key:
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\clsid
  Opens key:
                                  HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\protocol
  Opens key:
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\endpoint
  Opens key:
  Opens key:
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties\log
  Opens key:
                                  HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties\log\size
  Opens key:
  Opens key:
                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mtxoci.dll
                                  HKLM\software\microsoft\msdtc\mtxoci
  Opens key:
  Opens key:
                                  HKLM\software\microsoft\windows nt\currentversion\cluster server
  Opens key:
                                  HKLM\software\microsoft\msdtc\security
                                  HKLM\system\currentcontrolset\control\asr
  Opens kev:
  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 kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
  Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens kev:
Opens kev:
Opens key:
Opens kev:
Opens kev:
Opens key:
                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\svchost.exe
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
  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
                                  HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\svcid
  Opens key:
  Opens key:
                                  HKCR\svcid\6407e780-7e5d-11d0-8ce6-00c04fdc877e
  Opens key:
                                  HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\host
                                  HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\clsid
  Opens key:
  Opens key:
                                  HKCR \setminus svcid \setminus 6407e780-7e5d-11d0-8ce6-00c04fdc877e \setminus default provider
  Opens key:
                                  HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\protocol
                                  HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\endpoint
  Opens key:
  Opens key:
                                  HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896
  Opens key:
                                  HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\description
                                  HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\svcid
  Opens key:
  Opens key:
                                  HKCR\svcid\01366d42-c04e-11d1-b1c0-00c04fc2f3ef
                                  HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\host
  Opens kev:
  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 \verb|\| cid \verb|\| 2460f484-6eb1-4d02-91b6-690602ba23f9 \verb|\| custom properties \verb|\| log \verb|\| path | log \verb|\|
                                  HKU\.default\software\policies\microsoft\control panel\desktop
  Opens kev:
  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\currentcontrol\sa\sspicache\msapsspc.dll
Opens key: HKLM\system\currentcontrol\sa\sspicache\digest.dll
Opens key: HKLM\system\currentcontrol\sa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrol\set\control\sa\sspicache\msnsspc.dll
Opens key: HKLM\system\currentcontrol\set\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\

 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}\\reatas

 Opens key:
 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\\rinprocserver32

 Opens key:
 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\\rinprocserver32

 Opens key:
 HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\\rinprocserver32

 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}\inprochandler32

 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

```
HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\svcid
 Opens key:
 Opens key:
                         HKCR\svcid\ced2de40-bff6-11ce-9de8-00aa00a3f464
 Opens kev:
                         HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\host
                         HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\clsid
 Opens key:
 Opens kev:
                         HKCR\svcid\ced2de40-bff6-11ce-9de8-00aa00a3f464\defaultprovider
 Opens key:
                         HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\protocol
                         HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\endpoint
 Opens key:
                         HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\customproperties
 Opens key:
 Opens key:
                         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
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\treatas
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserver32
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprocserver32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserverx86
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\ inprocserverx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\localserver32
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\localserver32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprochandler32
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\\inprochandler32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprochandlerx86
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\localserver
                         HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\localserver
 Opens key:
 Opens key:
                         HKCU \setminus software \setminus classes \setminus clsid \setminus \{3bbe95da-c53f-11d1-b3a2-00a0c9083365\}
 Opens key:
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
 Opens key:
00a0c9083365}\treatas
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\treatas
 Opens kev:
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
 Opens key:
00a0c9083365}\inprocserver32
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
 Opens key:
00a0c9083365}\inprocserverx86
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
 Opens kev:
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
 Opens key:
00a0c9083365}\localserver32
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\localserver32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprochandler32
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\localserver
                         HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\localserver
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}
 Opens key:
 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
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprocserver32
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
 Opens kev:
00a0c9083365}\inprocserverx86
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\localserver32
 Opens key:
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\localserver32
                         HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
 Opens kev:
00a0c9083365}\inprochandler32
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprochandler32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
00a0c9083365}\inprochandlerx86
 Opens key:
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\) in prochandler x86
                         HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-
 Opens kev:
00a0c9083365}\localserver
                         HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\localserver
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}
                         HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-
00a0c9083365}\treatas
```

Opens key: $\label{local-b} $HKCR\clsid_{3bbe95d0-c53f-11d1-b3a2-00a0c9083365} \to \\ eats = \frac{1}{3} + \frac{1}{3$ 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: $\label{localserver32} \mbox{HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365\}\localserver32}}$

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}

00a0c9083365}\treatas

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

 $00600895e7d5 \} \verb|\inprocserverx86|$

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-

 $00600895e7d5 \} \\ local server$

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}

00a0c9083365}\treatas

Opens key: $\label{lem:hccn} \begin{tabular}{ll} HKCR\clsid\3bbe95f5-c53f-11d1-b3a2-00a0c9083365\treatas \\ Opens key: \\ HKCU\software\classes\clsid\3bbe95f5-c53f-11d1-b3a2-\\ \end{tabular}$

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 HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86 Opens kev: Opens key: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\localserver Opens kev: HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\localserver Opens key: HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-00a0c9083365} $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ca38d8da-c75d-11d1-8f99-00600895e7d5\}$ Opens key: HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5} Opens key: $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ca38d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8da-c75d-11d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d1-8f99-d8d8d-10d$ Opens key: 00600895e7d5}\treatas Opens kev: HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\treatas Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserver32 HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserver32 Opens key: Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserverx86 HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserverx86 Opens key: Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver32 HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprochandler32 HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprochandler32 Opens kev: Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprochandlerx86 HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprochandlerx86 Opens key: Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver Opens kev: Opens key: HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-00a0c9083365} Opens key: HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-00a0c9083365} HKLM\system\currentcontrolset\services\ipnat Opens key: Opens key: HKLM\system\currentcontrolset\services\ipnat\enum Opens key: HKLM\system\currentcontrolset\enum Opens key: Opens key: HKLM\system\currentcontrolset\hardware profiles\current Opens key: HKLM\system\currentcontrolset\hardware profiles\0001 HKLM\system\currentcontrolset\hardware Opens key: profiles\0001\system\currentcontrolset HKLM\system\currentcontrolset\hardware Opens key: profiles\0001\system\currentcontrolset\enum HKLM\system\currentcontrolset\hardware Opens key: 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] Oueries value: $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ [transparentenabled]$ HKCU\control panel\desktop[multiuilanguageid] Oueries value: Queries value: HKLM\software\microsoft\rpc[maxrpcsize] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: HKLM\system\wpa\mediacenter[installed] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [prioritize record data]$ HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata] Oueries value: $\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+dns \ cache \ \verb+parameters \ [allow un qualified query]$ Queries value: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [allow unqualified query]$ HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries 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[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]
 Oueries 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]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Oueries 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]
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
 Queries value:
                         HKLM\system\setup[systemsetupinprogress]
 Queries value:
HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[dnsquery time outs]|
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\gre_initialize[disablemetafiles]
                         HKLM\software\microsoft\windows nt\currentversion\compatibility32[msdtc]
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\ime
 Queries value:
compatibility[msdtc]
                         HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value:
                         HKLM\system\currentcontrolset\control\session
 Oueries value:
manager[criticalsectiontimeout]
 Queries value:
                         HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Queries value:
                          HKCR\interface[interfacehelperdisableall]
 Queries value:
                         HKCR\interface[interfacehelperdisableallforole32]
 Queries value:
                         HKCR\interface[interfacehelperdisabletypelib]
                         HKCR\interface\{00020400-0000-0000-c000-
 Oueries value:
00000000046}[interfacehelperdisableall]
                         HKCR\interface\{00020400-0000-0000-c000-
 Queries value:
00000000046}[interfacehelperdisableallforole32]
 Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                         HKLM\software\microsoft\msdtc[dtcenablelrm]
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\msdtc[rpcgoscapabilities]
 Oueries value:
                         HKLM\software\microsoft\msdtc[rpcqosidentity]
 Queries value:
                          HKLM\software\microsoft\msdtc[rpcauthnsvc]
 Oueries value:
                         HKLM\software\microsoft\msdtc[rpcauthnlevel]
```

HKLM\software\microsoft\msdtc[tracecmerr]

Queries value:

```
Oueries value:
                        HKLM\software\microsoft\msdtc[numcccimhistoryentries]
```

Oueries 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] Oueries value: HKLM\software\microsoft\msdtc[membuffersize] Oueries value: HKLM\software\microsoft\msdtc[cmcancelrpcafter] Oueries value: HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]

Oueries value: HKLM\software\microsoft\msdtc[cmmaxidlepings] HKLM\software\microsoft\msdtc[cmpingfreqsecs] Oueries value: Queries value: HKLM\software\microsoft\msdtc[cmverbose] Oueries value: HKLM\software\microsoft\msdtc[donotgoidle]

Oueries value: HKLM\software\microsoft\msdtc[allowonlysecurerpccalls] Queries value: HKLM\software\microsoft\msdtc[disablesinglephase]

Queries value: HKLM\software\microsoft\msdtc[usetiponly]

HKLM\software\microsoft\msdtc[createresourcemanagertimeout] Oueries value:

Queries value: HKLM\software\microsoft\msdtc[overridetiphostname]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Oueries 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] Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Oueries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 8]$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer31 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Oueries value: Oueries value: HKLM\software\microsoft\msdtc[turnoffbadmsgevents]

HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval] Queries value: Queries value: HKLM\software\microsoft\msdtc[xatmmaxwarmrecoveryinterval]

Oueries value: HKLM\software\microsoft\msdtc[tcpnodelay] HKLM\software\microsoft\msdtc[dtcmaxsessions] Queries value:

HKLM\software\microsoft\msdtc[disabletippassthrucheck] Oueries value: Oueries value: HKCU\software\microsoft\multimedia\audio[systemformats]

HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Queries value:

Queries value:

Oueries value:

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache] Queries value:

 $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. im ad pcm [cfilter tags]$

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\drivers32[msacm.msadpcm]

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]

Oueries value:

Oueries value:

 $HKLM \label{lem:hklm} \\ KLM \label{lem:hklm} HKLM \label{lem:hklm} \\ KLM \label{lem:hklm}$

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711] Oueries value: $HKLM \verb|\software\microsoft| audio compression manager \verb|\drivercache\mbox| msg711[fdw support]| and the support of the suppo$ Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags] Oueries value: Oueries value: $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox{|}msg711[cfiltertags]|$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msgsm610] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.trspch] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags] HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags] $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. msg723[aformattagcache]$ Oueries value: HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msaudio1] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cformattags]$ Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.sl_anet] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags] Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl_anet[a formattag cache]$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags] HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Queries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags] Oueries value: Oueries value: $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm.iac2 [cfilter tags]$ HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm] Oueries 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] Oueries value:

manager\msacm[nopcmconverter]
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority

HKCU\software\microsoft\multimedia\audio compression

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]

Queries value:

v4.00[priority1] HKCU\control panel\desktop[smoothscroll] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel] HKLM\software\microsoft\windows Oueries value: nt\currentversion\winlogon[chkaccdebuglevel] Oueries value: HKLM\system\currentcontrolset\control\productoptions[producttype] Oueries 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] Oueries 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] Oueries value: HKCU\control panel\international[locale] Queries value: HKLM\system\currentcontrolset\control\servicecurrent[] Queries value: HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes] Oueries 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[] HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\clsid[] Oueries value: Queries value: HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[] Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\protocol[] HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\endpoint[] Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-Queries value: 690602ba23f9\customproperties\log\size[] HKLM\software\microsoft\msdtc\mtxoci[oraclexalib] Oueries value: Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib] Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracleocilib] Queries value: HKLM\software\microsoft\msdtc\mtxoci[enabletrace] HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout] Queries value: Queries value: HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath] Oueries value: HKLM\software\microsoft\msdtc\mtxoci[debugtrace] HKLM\software\microsoft\msdtc\security[accountname] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version] 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] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries] Oueries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (000000000001[packed catalog item]) \ details \ de$ Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem] Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 000000000011 \ [packed catalog item]$ Queries value: $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 [serial_access_num]$ 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\00000000001[librarypath] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace] Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace_catalog S \setminus catalog_entries \setminus 000000000001[providerid]$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]

Queries value:

Queries value:

Oueries value:

```
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 0000000000001[version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000001[storesserviceclassinfo]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ (catalog\_entries \ 000000000002[library path])
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Oueries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus name space\_catalog 5 \setminus catalog\_entries \setminus 00000000000002 [address family]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 00000000000002 [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\00000000003[librarypath]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000003 \ [displaystring]
                                      HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\compatibility32[svchost]
                                     HKLM\software\microsoft\windows nt\currentversion\ime
  Queries value:
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\00000000003[addressfamily]
  Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000003 [supported name space]]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le catalog \le catalog \le catalog = not in the control set \setminus services \setminus catalog \le catalo
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
                                     HKLM\software\microsoft\msdtc\security[domaincontrollerstate]
  Queries value:
                                      HKLM\software\microsoft\msdtc\security[networkdtcaccess]
  Oueries value:
                                      HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
  Queries value:
  Queries value:
                                      HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
  Queries value:
                                      HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
  Oueries value:
                                      HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
  Queries value:
                                     HKLM\software\microsoft\msdtc\security[xatransactions]
  Oueries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:
                                      HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\description[]
                                      HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\description[]
  Queries value:
  Oueries value:
                                      HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\svcid[]
  Queries value:
                                      HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\host[]
                                      HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\clsid[]
  Oueries value:
                                      HKCR\svcid\6407e780-7e5d-11d0-8ce6-00c04fdc877e\defaultprovider[]
  Oueries value:
  Oueries value:
                                      HKU\.default\software\microsoft\multimedia\audio[systemformats]
                                      HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\protocol[]
  Queries value:
  Queries value:
                                      HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\endpoint[]
                                      HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\description[]
  Oueries value:
                                      HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\svcid[]
  Queries value:
  Queries value:
                                      HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\host[]
                                      HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\clsid[]
  Queries value:
                                      HKCR\svcid\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider[]
  Oueries value:
  Queries value:
                                      HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\protocol[]
  Oueries 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]
  Oueries value:
                                     HKU\.default\control panel\desktop[multiuilanguageid]
  Queries value:
                                     HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
  Oueries value:
                                     HKU\.default\control panel\desktop[smoothscroll]
  Queries value:
                                      HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[personal]
                                      HKU\.default\software\microsoft\windows\currentversion\explorer\user
  Oueries value:
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\currentcontrol\sa[everyoneincludesanonymous]

 Queries value:
 HKLM\system\currentcontrolset\services\eaphost\parameters[serviced1l]

 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:

 $HKLM \setminus system \setminus current control \setminus lsa \setminus sspicache \setminus msapsspc.dll[capabilities]$

Queries value: HKLM\system\currentcontrol\sa\sspicache\msapsspc.dll[rpcid]

Queries value:

HKLM\system\currentcontrol\sa\sspicache\msapsspc.dll[version]
Queries value: HKLM\system\currentcontrol\sa\sspicache\msapsspc.dll[type]

Oueries value:

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]

Queries value: HKLM\system\currentcontrol\sa\sspicache\digest.dll[name]
Queries value: HKLM\system\currentcontrol\set\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\currentcontrol\sa\sspicache\msnsspc.dll[name] Queries value: HKLM\system\currentcontrol\sa\sspicache\msnsspc.dll[comment]

Queries value:

 Queries value:
 HKLM\system\currentcontrol\sa\sspicache\msnsspc.dll[rpcid]

 Queries value:
 HKLM\system\currentcontrol\sa\sspicache\msnsspc.dll[version]

 Queries value:
 HKLM\system\currentcontrol\sa\sspicache\msnsspc.dll[type]

Queries value:

 $\label{thm:linear_quadratic} Queries \ value: \\ HKLM \ system \ current control \ value; \\ label{thm:linear_quadratic} HKLM \ system \ current control \ value; \\ label{thm:linear_quadratic} Algorithms \ label{thm:linear_quadratic} \\ label{thm:linear_quadratic} Queries \ value; \\ label{thm:linear_quadratic} Algorithms \ label{thm:linear_quadratic} \\ label{thm:linear_quadratic} Queries \ value; \\ label{thm:linear_quadratic} Queries \ value; \\ label{thm:linear_quadratic} Algorithms \ label{thm:linear_quadratic} Algorithms \ label{thm:linear_quadratic} \\ label{thm:linear_quadratic} Queries \ value; \\ label{thm:linear_quadratic} Queries \ value; \\ label{thm:linear_quadratic} Queries \ label{thm:linear_quadratic} \\ label{thm:linear_quadratic} Queries \ label{linear_quadratic} \\ label{thm:linear_quadratic} Queries \ label{linear_quadratic} \\ label{thm:linear_quadratic} Queries \ label{linear_quadratic} \\ label{thm:linear_quadratic} Queries \ label{l$

ab78-1084642581fb]

0000-0000000000000]

 Queries value:
 HKLM\system\currentcontrolset\services\eaphost\parameters[waithint]

 Queries value:
 HKLM\system\currentcontrolset\services\eaphost\parameters[peerinstalled]

Queries value:

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]

 $Queries \ value: \\ HKLM\ hardware\ description\ system\ central processor\ 0\ [\sim mhz]$

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:

Queries value:

 $HKLM \verb|\system| current controlset \verb|\services| rasman \verb|\ppp| eap \verb|\13[mppeen cryption supported]|$

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:

 $HKLM \verb|\system| current controlset \verb|\services| rasman| ppp \verb|\eap| 25[mppeen cryption supported]|$

Queries value:

```
HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[treatasmsmethod]
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[path]
   Oueries value:
   Oueries value:
                                              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[friendlyname]
   Queries value:
                                              HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[properties]
   Oueries value:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[configuipath]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[standalonesupported]
   Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[mppeencryptionsupported]
   Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[treatasmsmethod]
   Queries value:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[path]
   Oueries value:
                                              HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[friendlyname]
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[properties]
   Oueries value:
   Queries value:
                                             HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[configuipath]
   Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[standalonesupported]
   Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[mppeencryptionsupported]
   Oueries 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]
                                              HKLM\system\currentcontrolset\control\wmi\security[68fdd900-4a3e-11d1-
   Queries value:
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]
                                              HKLM\software\microsoft\com3[regdbversion]
   Oueries value:
   Queries value:
                                              HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[appid]
   Queries value:
                                              HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[dllsurrogate]
   Oueries 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]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\tracing\msdtc\modules[active]
                                             HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\tracing\msdtc\modules[level]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\tracing\msdtc\modules[controlflags]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\tracing\msdtc\modules\transaction_transitions[uniqueid]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\tracing\msdtc\modules\transaction_transitions[active]
   Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[level]
   Oueries value:
                                             HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions[controlflags]
                                              HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}[appid]
   Oueries value:
   Queries value:
                                              HKCR\appid\{8c482dce-2644-4419-aeff-189219f916b9}[dllsurrogate]
   Oueries value:
                                             HKCR\appid\{8c482dce-2644-4419-aeff-189219f916b9}[localservice]
                                              \label{local-eq:hkcr} $$ HKCR \inf \{ 7ed70824-03ad-41c1-ab1a-950621776881 \} \cap \{ 2eq. \} $$ (a) $$ (b) $$ (b) $$ (b) $$ (c) 
   Queries value:
   Oueries value:
                                             HKCR\clsid\{1510fb87-5676-40b9-a227-
5d0b66866f81}\inprocserver32[inprocserver32]
                                             HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprocserver32[]
   Queries value:
   Queries value:
                                              HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}[appid]
                                             HKCR\clsid\{1510fb87-5676-40b9-a227-
   Oueries value:
5d0b66866f81}\inprocserver32[threadingmodel]
   Queries value:
                                             HKLM\software\microsoft\msdtc[servicenetworkprotocols]
   Oueries 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[]
   Oueries 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[]
                                             HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\endpoint[]
   Oueries value:
   Queries value:
                                             HKCR\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserver32[inprocserver32]
                                             \label{lem:hkcrclsid} $$ HKCR\clsid{f117831b-c052-11d1-b1c0-00c04fc2f3ef} \in $$ (17831b-c052-11d1-b1c0-00c04fc2f3ef) $$ (1783b-c052-11d1-b1c0-00c04fc2f3ef) $$ (1783b-c052-00c04fc2f3ef) $$ (1783b-c052-00c04fc2f3ef) $$ (1783b-c052-00c04fc2f3ef) $$ (1783b-c052-00c04fc2f3ef) $$ (1783b-c052-00c04fc2f3ef) $$ (1783b-c052-00c04fc2f5ef) $$ (1783b-c052-00c04fc2f5ef) $$ (1783b-c052-00c04fc2f5ef) $$ (
   Queries value:
   Queries value:
                                              HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef\}[appid]
   Oueries value:
                                             HKCR\clsid\{f117831b-c052-11d1-b1c0-
00c04fc2f3ef}\inprocserver32[threadingmodel]
   Queries value:
                                             HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-
00a0c9083365}\inprocserver32[inprocserver32]
                                             HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
   Queries value:
                                              HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}[appid]
   Oueries value:
   Oueries 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[]
```

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

Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes:
HKLM\system\currentcontrolset\enum\root\legacy_ipnat\0000\control[activeservice]