# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 5, Task ID: 15

Task ID: 15 Risk Level:

Date Processed: 2016-04-07 08:21:31 (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 2016-04-07 08:21:31 (UTC) Date Added:

PE32:win32 File Type: 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]

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: C:\WINDOWS\system32\svchost.exe [C:\WINDOWS\System32\svchost.exe -k

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]

SharedAccess [C:\WINDOWS\system32\svchost.exe -k netsvcs] Loads service:

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\MSDTC\_NAMED\_EVENT **\BaseNamedObjects\DINPUTWINMM** Creates event:

Creates event:

\BaseNamedObjects\userenv: User Profile setup event

\BaseNamedObjects\crypt32LogoffEvent Creates event:

 $\label{lem:baseNamedObjects} $$ \added{A48F1A32-A340-11D1-BC6B-00A0C90312E1} $$ \added{A48F1A32-A340-11D1-BC6B-00A0C90312E1}$ Creates semaphore:

# 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:

Opens: C:\Documents and Settings\Admin

C:\Documents and Settings\Admin\output.txt Opens: C:\WINDOWS\Prefetch\MSDTC.EXE-0E6E4AF7.pf Opens:

Opens: C:\WINDOWS\system32

C:\WINDOWS\system32\msdtctm.dll Opens: C:\WINDOWS\system32\dnsapi.dll Opens: Opens: C:\WINDOWS\system32\ws2\_32.dll C:\WINDOWS\system32\ws2help.dll Opens: C:\WINDOWS\system32\msdtclog.dll Opens: Opens: C:\WINDOWS\system32\msdtcprx.dll

```
C:\WINDOWS\system32\msvcp60.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\mtxclu.dll
                         C:\WINDOWS\system32\comres.dll
 Opens:
 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
                         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
 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
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
                         C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\WINDOWS\system32\mtxoci.dll
                         C:\WINDOWS\system32\MSDtc\trace\dtctrace.log
 Opens:
 Opens:
                         C:\WINDOWS\system32\MsDtc\Trace
 Opens:
                         C:\WINDOWS\system32\MsDtc\Trace\dtctrace.log
                         C:\WINDOWS\system32\clbcatq.dll
 Opens:
 Opens:
                         C:\WINDOWS\Registration\R00000000007.clb
 Opens:
                         C:\WINDOWS\system32\MsDtc
                         C:\WINDOWS\system32\MsDtc\MSDTC.LOG
 Opens:
 Opens:
                         C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
 Opens:
 Opens:
                         {\tt C:\WINDOWS\system32\ntmarta.dll}
 Opens:
                         C:\WINDOWS\system32\samlib.dll
 Opens:
                         C:\WINDOWS\system32\winlogon.exe
                         C:\WINDOWS\system32\xpsp2res.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\eapsvc.dll
 Opens:
                         C:\WINDOWS\system32\eapphost.dll
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\msasn1.dll
 Opens:
                         C:\WINDOWS\system32\rastls.dll
 Opens:
                         C:\WINDOWS\system32\raschap.dll
 Opens:
                         C:\WINDOWS\System32\drivers\etc\lmhosts
 Opens:
                         C:\WINDOWS\system32\drivers\ipnat.sys
                         C:\Documents and Settings\Admin\output.txt
 Writes to:
 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
```

### Windows Registry Events

Reads from:

Creates key:

Creates key:	
HKLM\system\currento	controlset\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\currento	controlset\control\mediaproperties\privateproperties\joystick
Creates key:	<pre>HKCU\software\microsoft\multimedia\audio</pre>
Creates key:	<pre>HKCU\software\microsoft\multimedia\audio compression manager\</pre>
Creates key:	<pre>HKCU\software\microsoft\multimedia\audio compression manager\msacm</pre>
Creates key:	<pre>HKCU\software\microsoft\multimedia\audio compression manager\priority</pre>
v4.00	
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio</pre>
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio compression manager\</pre>
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio compression</pre>
manager\msacm	
Creates key:	<pre>HKU\.default\software\microsoft\multimedia\audio compression</pre>
manager\priority v4.	.00
Creates key:	<pre>HKLM\software\microsoft\windows nt\currentversion\tracing</pre>

C:\WINDOWS\Registration\R00000000007.clb

HKLM\system\currentcontrolset\services\tcpip\parameters

HKLM\software\microsoft\windows Creates key:

nt\currentversion\tracing\microsoft\eapsvc

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

HKLM\system\currentcontrolset\services\eaphost\parameters Creates kev:

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

 $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + winlog on + current + version + version$ Opens key: HKLM\

Opens key:

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

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

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

HKLM\software\microsoft\rpc\pagedbuffers Opens key:

Opens key: HKLM\software\microsoft\rpc

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

options\toggleservice32.exe\rpcthreadpoolthrottle

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key:  $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ limage file execution$ 

options\msdtc.exe

Opens kev: HKLM\svstem\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

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

options\user32.dll

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

options\gdi32.dll Opens key:

options\ole32.dll HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens key:

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 options\wsock32.dll

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

Opens key: options\mtxclu.dll

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

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\netapi32.dll

Opens key: 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 kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\xolehlp.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\msdtctm.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shimeng.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: 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\svstem\currentcontrolset\services\tcpip\parameters Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll HKLM\system\currentcontrolset\control\error message instrument\ Opens key: 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 HKLM\software\microsoft\ole Opens key: Opens key: HKCR\interface HKCR\interface\{00020400-0000-0000-c000-00000000046} Opens key: HKLM\system\currentcontrolset\control\computername Opens key: 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 HKI M\software\microsoft\msdtc Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\misc Opens key: HKLM\software\microsoft\xaincptr\two\_pipe\_trace  $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32$ Opens key: Opens kev: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm HKLM\software\microsoft\oleaut Opens key: Opens key: HKLM\software\microsoft\oleaut\userera HKLM\software\microsoft\audiocompressionmanager\drivercache Opens kev: Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.im aadpcm$ Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msadpcm$  $HKLM \ \ software \ \ \ microsoft \ \ \ audio compression manager \ \ \ \ msg711$ Opens key: Opens kev:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msgsm610$  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ trspch$ Opens key: Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723 Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msaudio 1$ Opens key:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.sl\_anet$ Opens key:  $HKLM \verb|\software\microsoft\audiocompression manager \verb|\drivercache\msacm.iac2| \\$ Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm HKLM\system\currentcontrolset\control\mediaresources\acm Opens key: Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance Opens key:  $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} If the lem is a simple constant of the lem is a simple constant$ Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ advanced$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack Opens key: HKLM\system\currentcontrolset\control\productoptions  $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ explorer\+ user shell$ Opens key: folders HKLM\software\policies\microsoft\windows\system Opens kev:  $\label{thm:local_equation} \parbox{$HKCU\software\microsoft\windows\currentversion\thememanager} \\$ Opens key: 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 HKLM\software\classes Opens key:

Opens key: HKCR\cid

```
HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9
 Opens key:
 Opens key:
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\description
 Opens kev:
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\svcid
 Opens key:
 Opens key:
                     HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464
 Opens key:
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\host
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\clsid
 Opens key:
 Opens key:
                     HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider
 Opens key:
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\protocol
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\endpoint
 Opens key:
 Opens key:
                     HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\customproperties
 Opens key:
                     HKCR \verb|\cid|| 2460f484-6eb1-4d02-91b6-690602ba23f9 \verb|\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
                     HKI M\software\microsoft\windows nt\currentversion\cluster server
 Opens kev:
 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 kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens kev:
Opens kev:
Opens kev:
Opens kev:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
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
 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
                     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:
                     \label{local-equation} HKCR \land 2460f484-6eb1-4d02-91b6-690602ba23f9 \land custom properties \land log \land path \end{substitute}
 Opens key:
                     HKLM\software\microsoft\rpc\securityservice
 Opens key:
                     {\it HKLM \ } system \ `current control \ `security providers
```

```
HKLM\system\currentcontrolset\control\lsa\sspicache
 Opens key:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
 Opens key:
                         HKLM \ system \ current control \ lsa \ spicache \ digest. dll
 Opens kev:
 Opens key:
                         HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
 Opens kev:
                         HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
 Opens key:
                         HKLM\system\currentcontrolset\control\wmi\security
                         HKLM\software\microsoft\windows
 Opens key:
nt\currentversion\tracing\msdtc\loggingoptions
 Opens key:
                         HKLM\hardware\description\system\centralprocessor\0
                         HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\modules
 Opens key:
 Opens kev:
                         HKLM\software\microsoft\windows
nt\currentversion\tracing\msdtc\modules\transaction_transitions
                         HKLM\software\microsoft\windows nt\currentversion\tracing\msdtc\changed
                         HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\svcid
 Opens key:
 Opens key:
                         HKCR\svcid\ced2de40-bff6-11ce-9de8-00aa00a3f464
```

 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:  $\label{eq:hkcr} \begin{tabular}{ll} HKCR \cid\a0605a20-8d7d-4181-81f4-3318a962135c\customproperties \\ Opens key: \\ HKCR \cid\a0605a20-8d7d-4181-81f4-3318a962135c\customproperties \dac \\ \end{tabular}$ 

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:  $\label{eq:hccu} \begin{tabular}{ll} HKCU\software\classes\clsid\f117831b-c052-11d1-b1c0-00c04fc2f3ef} \end{tabular}$ 

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

 $Opens~key: \\ HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\\\ \label{eq:c1} inprocserverx86$ 

Opens key: HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-

 $00c04fc2f3ef} \\ \\ localserver 32$ 

Opens key: HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\localserver32

Opens key: HKCU\software\classes\clsid\{f117831b-c052-11d1-b1c0-

 $00c04fc2f3ef \verb|\inprochandler32|$ 

 $Opens~key: \\ HKCR\clsid\{f117831b-c052-11d1-b1c0-00c04fc2f3ef}\inprochandler 32$ 

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}

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

HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86 Opens key:

HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-Opens key:

00a0c9083365}\localserver32

Opens key:  $HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\localserver 32$ 

HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-Opens key:

00a0c9083365}\inprochandler32

 $\label{lem:hkcr} $$HKCR\clsid{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\inprochandler 32 $$$ Opens key:

HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-Opens key:

00a0c9083365}\inprochandlerx86

 $HKCR\clsid\{3bbe95a4-c53f-11d1-b3a2-00a0c9083365}\) in prochandler x86$ Opens key:

Opens key: HKCU\software\classes\clsid\{3bbe95a4-c53f-11d1-b3a2-

00a0c9083365}\localserver

Opens key:  $\label{localserver} $HKCR \cdot 1 - b3a2 - 00a0c9083365 \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - b3a2 - 00a0c9083365) \cdot 10calserver $$ (3bbe95a4 - c53f - 11d1 - c53f - c54f - c54f$ HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365} Opens key:

HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365} Opens kev:

Opens key: HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-

00a0c9083365}\treatas

HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-

00a0c9083365}\inprocserver32

HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-

00a0c9083365}\inprocserverx86

HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86 Opens key:

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

 $HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\\\\inprochandler32$ Opens key:

Opens key: HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-

00a0c9083365}\inprochandlerx86

HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{3bbe95d0-c53f-11d1-b3a2-

00a0c9083365}\localserver

HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\localserver Opens key:

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

HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\treatas Opens kev: HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-Opens key:

00a0c9083365}\inprocserver32

HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprocserver32 Opens key:

HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-Opens key:

00a0c9083365}\inprocserverx86

HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86 Opens kev:

Opens key: HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-

00a0c9083365}\localserver32

HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-

00a0c9083365}\inprochandler32

HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprochandler32 Opens kev:

Opens key: HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-

00a0c9083365}\inprochandlerx86

HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86 Opens key:

HKCU\software\classes\clsid\{3bbe95df-c53f-11d1-b3a2-Opens key:

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}

HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5} Opens kev: Opens key: HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-

00600895e7d5}\treatas

Opens key: HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\treatas HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-Opens key:

00600895e7d5}\inprocserver32

HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprocserver32 Opens kev:

Opens key: HKCU\software\classes\clsid\{5408b2f0-c816-11d1-8f99-

00600895e7d5}\inprocserverx86

Opens key: HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprocserverx86

Opens key:

00600895e7d5}\localserver32

HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\localserver32 Opens kev:

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

HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprochandlerx86 Opens kev:

Opens key:  00600895e7d5}\localserver Opens key: HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\localserver HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365} Opens key: Opens key: HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365} Opens kev: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\treatas HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprocserver32 HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprocserver32 Opens key: Opens kev: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprocserverx86 Opens key:  $\label{lem:hkcr} $$ HKCR\clsid_{3bbe95f5-c53f-11d1-b3a2-00a0c9083365} \in \cline{100} $$ HKCR_{clsid}_{3bbe95f5-c53f-11d1-b3a2-00a0c9083365} \in \cline{100} $$ HKCR_{clsid}_{3bbe95f5-c53f-11d1-b3a2-00a0c908365} \in \cline{100} $$ HKCR_{clsid}_{3bbe95f5-c53$ HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-Opens key: 00a0c9083365}\localserver32 HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\localserver32 Opens key: Opens key: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprochandler32 Opens key:  $HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\tinprochandler 32$ Opens key: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86 HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\inprochandlerx86 Opens key: HKCU\software\classes\clsid\{3bbe95f5-c53f-11d1-b3a2-Opens kev: 00a0c9083365}\localserver Opens key: HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-00a0c9083365}\localserver HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-00a0c9083365} Opens key: Opens key:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{ca38d8da-c75d-11d1-8f99-00600895e7d5\}$ HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5} Opens key: HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-Opens kev: 00600895e7d5}\treatas Opens key: HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\treatas HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-Opens key: 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 HKCU\software\classes\clsid\{ca38d8da-c75d-11d1-8f99-Opens key: 00600895e7d5}\localserver HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\localserver Opens kev: HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-00a0c9083365} Opens key: Opens key: HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-00a0c9083365} Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\svchost.exe Opens key: HKU\.default\software\policies\microsoft\control panel\desktop Opens key: HKU\.default\control panel\desktop  $HKU \verb|\|.default\| software \verb|\| microsoft\| windows \verb|\| current version \verb|\| explorer \verb|\| advanced | leaves to be a constraint of the constraint of the$ Opens key: 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 HKLM\system\currentcontrolset\control\lsa Opens key: Opens key: HKLM\system\currentcontrolset\services Opens key: HKLM\system\currentcontrolset\services\eaphost Opens key: HKLM\system\currentcontrolset\services\eaphost\parameters

Opens key:

```
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\system\currentcontrolset\services\eaphost\methods
   Opens kev:
                                                HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}
   Opens key:
                                                HKCR \verb|\clsid|{0a886f29-465a-4aea-8b8e-be926bfae83e} \verb|\treatas|
   Opens key:
   Opens key:
                                                HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\inprocserver32
   Opens key:
                                                HKCR \clsid \ \{0a886f29-465a-4aea-8b8e-be926bfae83e\} \label{linprocserverx86}
                                                HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\localserver32
   Opens key:
                                                HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\tinprochandler32
   Opens key:
   Opens key:
                                                HKCR \verb|\clsid|{0a886f29-465a-4aea-8b8e-be926bfae83e} \verb|\inprochandlerx86||
   Opens key:
                                                HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}\localserver
                                                HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}
   Opens key:
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\treatas
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprocserver32
   Opens kev:
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprocserverx86
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\localserver32
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\inprochandler32
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\tinprochandlerx86
   Opens key:
                                                HKCR\clsid\{8c482dce-2644-4419-aeff-189219f916b9}\localserver
                                                HKCR\appid\{8c482dce-2644-4419-aeff-189219f916b9}
   Opens kev:
   Opens key:
                                                HKCR\interface\{7ed70824-03ad-41c1-ab1a-950621776881}
   Opens key:
                                                HKCR \land (7ed70824-03ad-41c1-ab1a-950621776881) \land (proxystubclsid32) \land (
   Opens key:
                                                HKCR \ clsid \ \{1510fb87 - 5676 - 40b9 - a227 - 5d0b66866f81\}
   Opens key:
                                                HKCR \clsid \ \{1510fb87-5676-40b9-a227-5d0b66866f81\} \ treat as
   Opens key:
                                                HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprocserver32
                                                \label{lem:hkcr} $$ HKCR\clsid_{1510fb87-5676-40b9-a227-5d0b66866f81} \in \clsid_{1510fb87-5676-40b9-a227-5d0b66866f81} $$ inprocessing the second of the se
   Opens key:
   Opens key:
                                                HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\localserver32
   Opens key:
                                                HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprochandler32
                                                HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprochandlerx86
   Opens key:
   Opens key:
                                                HKCR \ clsid \ \{1510fb87-5676-40b9-a227-5d0b66866f81\} \ local server
   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
                                                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]
   Oueries 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\codeidentifiers[transparentenabled]
                                                HKCU\control panel\desktop[multiuilanguageid]
   Oueries value:
   Oueries value:
                                                HKLM\software\microsoft\rpc[maxrpcsize]
                                                HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:
   Queries value:
                                                HKLM\system\wpa\mediacenter[installed]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [allow unqualified query]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Oueries 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]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:
                                                HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
```

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus trpip \setminus parameters [enable adapter domain name registration]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries 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:  $HKLM \backslash system \backslash current control set \backslash services \backslash tcpip \backslash parameters [default registration refreshinter val]$ 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] HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel] Oueries value: HKLM\system\setup[systemsetupinprogress] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Oueries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquick query time outs]$ HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts] Oueries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles] HKLM\software\microsoft\windows nt\currentversion\compatibilitv32[msdtc] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibilitv[msdtc] Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls] Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout] HKLM\software\microsoft\ole[rwlockresourcetimeout] Oueries value: Queries value: HKCR\interface[interfacehelperdisableall] HKCR\interface[interfacehelperdisableallforole32] Oueries value: Oueries value: HKCR\interface[interfacehelperdisabletypelib] HKCR\interface\{00020400-0000-0000-c000-Queries value: 00000000046}[interfacehelperdisableall] HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableallforole32] Oueries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername] Oueries value: HKLM\software\microsoft\msdtc[dtcenablelrm] Queries value: HKLM\software\microsoft\msdtc[rpcqoscapabilities] HKLM\software\microsoft\msdtc[rpcqosidentity] Oueries value:

HKLM\software\microsoft\msdtc[rpcauthnsvc]

Queries value:

```
Oueries value:
                          HKLM\software\microsoft\msdtc[rpcauthnlevel]
 Oueries value:
                          HKLM\software\microsoft\msdtc[tracecmerr]
 Oueries 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]
                          HKLM\software\microsoft\msdtc[dtcmemalloc1
 Oueries value:
 Oueries value:
                          HKLM\software\microsoft\msdtc[membuffersize]
 Oueries value:
                          HKLM\software\microsoft\msdtc[cmcancelrpcafter]
 Oueries value:
                          HKLM\software\microsoft\msdtc[cmmaxnumberbindretries]
 Queries value:
                          HKLM\software\microsoft\msdtc[cmmaxidlepings]
 Oueries value:
                          HKLM\software\microsoft\msdtc[cmpingfreqsecs]
 Oueries value:
                          HKLM\software\microsoft\msdtc[cmverbose]
 Queries value:
                          HKLM\software\microsoft\msdtc[donotgoidle]
 Queries value:
                          HKLM\software\microsoft\msdtc[allowonlysecurerpccalls]
 Oueries value:
                          HKLM\software\microsoft\msdtc[disablesinglephase]
 Queries value:
                          HKLM\software\microsoft\msdtc[usetiponly]
 Oueries value:
                          HKLM\software\microsoft\msdtc[createresourcemanagertimeout]
 Oueries 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]
 Oueries 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]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
 Oueries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
 Queries value:
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
 Queries value:
 Oueries value:
                          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Oueries value:
 Queries value:
 Queries value:
 Oueries value:
 Queries value:
 Oueries value:
 Oueries value:
 Oueries value:
 Queries value:
 Oueries value:
 Queries value:
 Oueries value:
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]  $HKLM \setminus software \setminus microsoft \setminus windows \ nt \setminus current version \setminus drivers 32 [aux 6]$ HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Queries value:

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

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]

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

Oueries value: HKLM\software\microsoft\msdtc[xatmminwarmrecoveryinterval]  ${\it HKLM} \verb|\software\microsoft\mbox{|} msdtc[xatmmaxwarmrecoveryinterval]|}$ Queries value:

Oueries value: HKLM\software\microsoft\msdtc[tcpnodelav] Oueries value: HKLM\software\microsoft\msdtc[dtcmaxsessions]

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.imaadpcm]

Oueries value:

Oueries value:

Oueries value:

Queries value:

Queries value:

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

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

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.ima adpcm [cfilter tags]$ 

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msadpcm]

Oueries value:

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

Oueries value:

 $HKLM \verb| software \verb| microsoft| audio compression manager \verb| driver cache \verb| msadpcm[cformattags]| \\$ 

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msg711] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags] Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msg 711 [a formattag cache]$ Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. msg711[cfilter tags]$ HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.msgsm610] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport] Oueries value:  $\label{thm:macmmag} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} microsoft \end{tabular} audio compression manager \end{tabular} driver cache \end{tabular} macm. msgsm610 [cformattags] \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} for each end of the compression manager \end{tabular} audio compression manager \end{tabular} audio com$ HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags] HKLM\software\microsoft\windows Queries value: nt\currentversion\drivers32[msacm.trspch] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg723] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags] Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. msg 723 [a formattag cache]$ Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \\ msg723[cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msaudio1] Oueries value: Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audiocompression manager \setminus driver cache \setminus msacm. msaudio1[cformattags]$ Oueries value:  $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msaudio1 \lceil aformattag cache \rceil$ Queries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msaudio1[cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.sl\_anet] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[fdwsupport] Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. sl\_anet [cformattags]$ Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[aformattagcache] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cfiltertags] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport] Oueries value: Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msacm. iac 2 [a formattag cache]$ 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.13acm[fdwsupport] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags] Oueries value:

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

HKCU\software\microsoft\multimedia\audio compression

 $HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} I3 acm [cfilter tags] \\$ 

Queries value:

Queries value:

manager\msacm[nopcmconverter] HKCU\software\microsoft\multimedia\audio compression manager\priority Oueries value: v4.00[priority1] Queries value: HKCU\control panel\desktop[smoothscroll] HKLM\software\microsoft\windows Oueries value: 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsopdebuglevel] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] HKCU\software\microsoft\windows\currentversion\thememanager[compositing] Oueries value: Queries value: HKCU\control panel\desktop[lamebuttontext] Queries value: HKCU\control panel\international[locale] Oueries value: HKLM\system\currentcontrolset\control\servicecurrent[] Queries value: HKLM\software\microsoft\msdtc[maxrecoverytimepermbinminutes] Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\description[] HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\svcid[] Oueries value: Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\host[] Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\clsid[] HKCR\svcid\488091f0-bff6-11ce-9de8-00aa00a3f464\defaultprovider[] Queries value: Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\protocol[] Queries value: HKCR\cid\2460f484-6eb1-4d02-91b6-690602ba23f9\endpoint[] HKCR\cid\2460f484-6eb1-4d02-91b6-Oueries value: 690602ba23f9\customproperties\log\size[] Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclexalib] Queries value: HKLM\software\microsoft\msdtc\mtxoci[oraclesqllib] HKLM\software\microsoft\msdtc\mtxoci[oracleocilib] Queries value: Queries value: HKLM\software\microsoft\msdtc\mtxoci[enabletrace] Oueries value: HKLM\software\microsoft\msdtc\mtxoci[mtxocicptimeout] HKLM\software\microsoft\msdtc\mtxoci[oracletracefilepath] Queries value: HKLM\software\microsoft\msdtc\mtxoci[debugtrace] Oueries value: Oueries value: HKLM\software\microsoft\msdtc\security[accountname] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num] Oueries 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] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000001[packedcatalogitem] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000003[packedcatalogitem] Queries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005[packedcatalogitem] Oueries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[packedcatalogitem] Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000009[packedcatalogitem] 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\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[displaystring] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerid]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[addressfamily]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[supportednamespace]

Oueries value:

Queries value:

Queries value:

```
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
   Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ name space\_catalog \ nam
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus catalog\_entries \setminus 0000000000002[supported names pace]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 00000000000002 [enabled]
   Queries value:
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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
   Queries value:
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000003 \ [address family]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
   Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap services \setminus catalog \le ca
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock2 \setminus parameters [ws2\_32 spin count]
                                               HKLM\software\microsoft\msdtc\security[domaincontrollerstate]
   Queries value:
   Oueries value:
                                               HKLM\software\microsoft\msdtc\securitv[networkdtcaccess]
   Queries value:
                                               HKLM\software\microsoft\msdtc\security[networkdtcaccessadmin]
                                               HKLM\software\microsoft\msdtc\security[networkdtcaccessclients]
   Oueries value:
   Queries value:
                                               HKLM\software\microsoft\msdtc\security[networkdtcaccesstransactions]
   Oueries value:
                                               HKLM\software\microsoft\msdtc\security[networkdtcaccesstip]
                                               {\it HKLM} \verb|\software\m| icrosoft\m| sdtc\security[xatransactions]
   Queries value:
   Oueries value:
                                               HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\description[]
   Queries value:
                                               HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\description[]
                                               HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\svcid[]
   Oueries value:
                                               HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\host[]
   Oueries value:
   Queries value:
                                               HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\clsid[]
   Queries value:
                                               HKCR \setminus svcid \setminus 6407e780-7e5d-11d0-8ce6-00c04fdc877e \setminus defaultprovider[]
   Oueries value:
                                               HKCR\cid\e72de59b-5bb7-496b-a0f7-4a11bd519654\protocol[]
   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[]
   Oueries value:
                                               HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\host[]
   Oueries value:
                                               HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\clsid[]
   Queries value:
   Queries value:
                                               HKCR\svcid\01366d42-c04e-11d1-b1c0-00c04fc2f3ef\defaultprovider[]
   Oueries value:
                                               HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\protocol[]
                                               HKCR\cid\e743c464-3401-4931-ab4a-d71b8b9d3896\endpoint[]
   Queries value:
   Queries value:
                                               HKCR\cid\2460f484-6eb1-4d02-91b6-
690602ba23f9\customproperties\log\path[]
                                              HKLM\software\microsoft\rpc\securityservice[9]
   Oueries value:
   Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
   Queries value:
                                               manager[safeprocesssearchmode]
   Queries value:
                                               HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
   Oueries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
```

Queries value:

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

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid] Oueries value:

Queries value:

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

HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type] Oueries value:

Oueries value:

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

HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name] Oueries value: 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\currentcontrol\sa\sspicache\digest.dll[rpcid]
Queries value: HKLM\system\currentcontrol\sa\sspicache\digest.dll[version]
Queries value: HKLM\system\currentcontrol\sa\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\currentcontrol\sa\sspicache\msnsspc.dll[rpcid]

 Queries value:
 HKLM\system\currentcontrol\set\control\lsa\sspicache\msnsspc.dll[version]

 Queries value:
 HKLM\system\currentcontrol\set\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-

0000-00000000000001

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\system\currentcontrolset\control\wmi\security[68fdd900-4a3e-11d1-

84f4-0000f80464e3]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[5b6f6eeb-8fb8-42b8-

8e8d-f0f9a3d3f1a7]

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

 $\verb|nt\currentversion\tracing\msdtc\modules\transaction\_transitions[active]|$ 

Queries value: HKLM\software\microsoft\windows

 $\verb| nt\current version \verb| tracing \verb| msdtc \verb| modules \verb| transaction_transitions[level]| \\$ 

Queries value: HKLM\software\microsoft\windows

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[]

nt\currentversion\tracing\msdtc\modules\transaction\_transitions[controlflags]

Queries value: HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\host[]
Queries value: HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\host[]
Queries value: HKCR\cid\a0605a20-8d7d-4181-81f4-3318a962135c\clsid[]
Oueries 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\protocol[]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKLM\software\microsoft\com3[regdbversion] Queries value: HKCR\clsid\{f117831b-c052-11d1-b1c0-

00c04fc2f3ef}\inprocserver32[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]

 $Queries\ value: \\ HKCR\clsid\{3bbe95da-c53f-11d1-b3a2-00a0c9083365}\\\ \ linprocserver32[]$ 

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[]

 $Queries\ value: \ HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-00a0c9083365}\ [appid]$ 

```
HKCR\clsid\{3bbe95d0-c53f-11d1-b3a2-
 Oueries value:
00a0c9083365}\inprocserver32[threadingmodel]
                          HKLM\software\microsoft\msdtc[transactionbridge]
 Oueries value:
                          HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-
 Queries value:
00a0c9083365}\inprocserver32[inprocserver32]
 Queries value:
                          HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}\inprocserver32[]
                          HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-00a0c9083365}[appid]
 Oueries value:
                          HKCR\clsid\{3bbe95df-c53f-11d1-b3a2-
 Oueries value:
00a0c9083365}\inprocserver32[threadingmodel]
                          HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-
 Oueries value:
00a0c9083365}[interfacehelperdisabletypelib]
 Queries value:
                          HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisableall]
                         HKCR\interface\{3bbe95f0-c53f-11d1-b3a2-
 Oueries value:
00a0c9083365}[interfacehelperuser]
 Queries value:
                         HKCR\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprocserver32[inprocserver32]
                          HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}\inprocserver32[]
 Queries value:
 Queries value:
                          HKCR\clsid\{5408b2f0-c816-11d1-8f99-00600895e7d5}[appid]
 Oueries value:
                         HKCR\clsid\{5408b2f0-c816-11d1-8f99-
00600895e7d5}\inprocserver32[threadingmodel]
 Oueries 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]
                         HKCR\clsid\{3bbe95f5-c53f-11d1-b3a2-
 Queries value:
00a0c9083365}\inprocserver32[threadingmodel]
 Queries value:
                          HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisabletypelib]
                          HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-
 Queries value:
00a0c9083365}[interfacehelperdisableall]
                         HKCR\interface\{3bbe95f3-c53f-11d1-b3a2-
 Queries value:
00a0c9083365}[interfacehelperuser]
 Queries value:
                         HKCR\clsid\{ca38d8da-c75d-11d1-8f99-
00600895e7d5}\inprocserver32[inprocserver32]
                          HKCR\clsid\{ca38d8da-c75d-11d1-8f99-00600895e7d5}\inprocserver32[]
 Queries 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-
 Queries value:
00a0c9083365}[interfacehelperdisableall]
                         HKCR\interface\{3bbe95f4-c53f-11d1-b3a2-
 Queries value:
00a0c9083365}[interfacehelperuser]
                         HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-
 Queries value:
00a0c9083365}[interfacehelperdisabletypelib]
 Queries value:
                         HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperdisableall]
 Queries value:
                         HKCR\interface\{3bbe95d6-c53f-11d1-b3a2-
00a0c9083365}[interfacehelperuser]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[svchost]
 Queries value:
                          HKLM\software\microsoft\windows nt\currentversion\ime
compatibilitv[svchost]
 Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                          HKU\.default\software\microsoft\multimedia\audio[systemformats]
 Oueries value:
                          HKU\.default\software\microsoft\multimedia\audio compression
 Oueries value:
manager\msacm[nopcmconverter]
 Queries value:
                         HKU\.default\control panel\desktop[multiuilanguageid]
 Oueries value:
                         HKU\.default\software\microsoft\multimedia\audio compression
manager\priority v4.00[priority1]
                          HKU\.default\control panel\desktop[smoothscroll]
 Oueries value:
 Queries value:
                          HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[personal]
                          HKU\.default\software\microsoft\windows\currentversion\explorer\user
 Queries value:
shell folders[local settings]
 Queries value:
HKU\.default\software\microsoft\windows\currentversion\thememanager[compositing]
 Queries value:
                          HKU\.default\control panel\desktop[lamebuttontext]
                          \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ svchost[eapsvcs]
 Oueries value:
 Oueries 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]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\svchost\eapsvcs[authenticationcapabilities]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\svchost\eapsvcs[defaultrpcstacksize]
 Queries value:
                          HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
```

```
HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Oueries value:
  Oueries value:
                                   HKLM\system\currentcontrolset\services\eaphost\parameters[servicedll]
  Queries value:
                                   HKLM\system\currentcontrolset\services\eaphost\parameters[servicemain]
  Oueries value:
                                   {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ eaphost \verb|\ parameters [waithint]|
  Queries value:
                                   HKLM\system\currentcontrolset\services\eaphost\parameters[peerinstalled]
  Oueries value:
HKLM\system\currentcontrolset\services\eaphost\parameters[authenticatorinstalled]
                                   Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[properties]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[configuipath]
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[standalonesupported]
  Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[mppeencryptionsupported]
  Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[treatasmsmethod]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\13[path]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[friendlyname]
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[properties]
  Oueries value:
  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]
  Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[treatasmsmethod]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\25[path]
                                   HKLM \setminus system \setminus current control set \setminus services \setminus rasman \setminus ppp \setminus 26[friendly name]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[properties]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[configuipath]
  Oueries 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]
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\26[path]
  Oueries value:
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[friendlyname]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[properties]
                                   Oueries value:
  Queries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[standalonesupported]
  Oueries value:
HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[mppeencryptionsupported]
  Queries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[treatasmsmethod]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\rasman\ppp\eap\4[path]
  Queries value:
                                   HKCR\clsid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[appid]
  Queries value:
                                   HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[dllsurrogate]
                                   HKCR\appid\{0a886f29-465a-4aea-8b8e-be926bfae83e}[localservice]
  Oueries value:
                                   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} $$ HKCR \inf \{ 7ed70824 - 03ad - 41c1 - ab1a - 950621776881 \} \cap S(32[]) $$ is the substitution of the sub
  Queries value:
  Oueries value:
                                   HKCR\clsid\{1510fb87-5676-40b9-a227-
5d0b66866f81}\inprocserver32[inprocserver32]
                                   HKCR\clsid\{1510fb87-5676-40b9-a227-5d0b66866f81}\inprocserver32[]
  Oueries 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\system\currentcontrolset\services\ipnat[imagepath]
  Oueries value:
                                   HKLM\system\currentcontrolset\services\ipnat[objectname]
  Queries value:
                                   HKLM\system\currentcontrolset\services\ipnat[type]
  Queries value:
                                   HKLM\system\currentcontrolset\services\ipnat\enum[count]
                                   HKLM\system\currentcontrolset\services\ipnat\enum[0]
  Oueries value:
                                   HKLM\system\currentcontrolset\enum\root\legacy_ipnat\0000[configflags]
  Oueries value:
  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]
                                   HKLM\software\microsoft\windows
  Sets/Creates value:
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]
```

HKLM\software\microsoft\windows

Sets/Creates value:

nt\currentversion\tracing\microsoft\eapphost\traceidentifier[guid]

Sets/Creates value: HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eapphost\traceidentifier[bitnames] HKLM\software\microsoft\cryptography\rng[seed] Value changes:

Value changes:

HKLM\system\currentcontrolset\enum\root\legacy\_ipnat\0000\control[activeservice]