## Malware Analysis Appliance by Blue Coat Systems, Inc.

# Task Details

mag2, Sample ID: 3331, Task ID: 832

Task ID: Risk Level: 10

Date Processed: 2016-05-18 10:44:05 (UTC)

Processing Time: Virtual Environment: 62.2 seconds

"c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe' Execution Arguments:

Sample ID: 3331 Type: basic admin Owner:

Label: 1be5bc13fd1cf615a95feec0c5b7fd13 Date Added 2016-05-18 10:30:52 (UTC)

File Type: PE32:win32:gui File Size 201728 bytes

1be5bc13fd1cf615a95feec0c5b7fd13

SHA256: 10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347

Description:

#### Pattern Matching Results

Modifies registry autorun entries Writes to memory of system processes

5 Abnormal sleep detected

Installs service 3 Connects to local host

Creates file in recycle bin

Changes Winsock providers

Creates malicious events: ZeroAccess [Rootkit]

4 Reads process memory

Opens a recycle bin location

Creates threads in system processes

3 Long sleep detected

Injects thread into Windows process

#### Process/Thread Events

Creates process: C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe

["c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"]

Creates process: C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe"]

Reads from process: PID:1988 C:\WINDOWS\system32\calc.exe

PID:1900 C:\WINDOWS\explorer.exe
PID:896 C:\WINDOWS\system32\services.exe Writes to process: Writes to process: Writes to process:

PID:640 C:\WINDOWS\system32\cmd.exe C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe Terminates process:

Creates remote thread: C:\WINDOWS\explorer.exe

C:\WINDOWS\system32\services.exe Creates remote thread:

#### Named Object Events

\BaseNamedObjects\SHIMLIB\_LOG\_MUTEX
\BaseNamedObjects\MSCTF.Shared.MUTEX.EHH Creates mutex:

Creates mutex Creates event: Creates event:

\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}\BaseNamedObjects\userenv: User Profile setup event Creates event: Creates event:

Creates event

\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000007B4.00000000.00000004

\BaseNamedObjects\CTF.ThreadMTConnectionEvent.000007B4.00000000.00000004 Creates event

\BaseNamedObjects\MSCTF.SendReceive.Event.ELH.IC \BaseNamedObjects\MSCTF.SendReceiveConection.Event.ELH.IC Creates event: Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.EHH.IC \BaseNamedObjects\MSCTF.SendReceiveConection.Event.EHH.IC Creates event: Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

#### File System Events

Creates C:\RECYCLER

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003 C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-Creates

1003\\$685c83111e534ea0f6bc8e25bc965f78 Creates: C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\L Creates: C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-1003\\$685c83111e534ea0f6bc8e25bc965f78\U

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\@

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\n C:\RECYCLER\ C:\RECYCLER\S-1-5-18 Creates

Creates

C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78 C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\L Creates Creates C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\U
C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\@ Creates Creates C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\n C:GAC\_MSIL

Creates

C:\WINDOWS\assembly\GAC
C:\WINDOWS\assembly\GAC\Desktop.ini Creates Creates

Opens:

C:\WINDOWS\Prefetch\1BE5BC13FD1CF615A95FEECOC5B7F-1D9D4140.pf C:\Documents and Settings\Admin Opens:

C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\cabinet.dll Opens: Opens Opens: C:\WINDOWS\system32\ws2\_32.dll C:\WINDOWS\system32\ws2help.dll Opens: C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll C:\WINDOWS\system32\rsaenh.dll Opens: Opens: C:\WINDOWS\system32\crypt32.dll

Opens: :\WINDOWS

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-Opens

1003\\$685c83111e534ea0f6bc8e25bc965f78

C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-

1003\\$685c83111e534ea0f6bc8e25bc965f78\n
Opens: C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78 C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\n C:\WINDOWS\assembly Opens:

Opens:

C:\WINDOWS\assembly\GAC\Desktop.ini Opens

```
Opens
                                     C:\WTNDOWS\assemblv\GAC
                                     C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\apphelp.dll
  Opens:
  Opens:
                                     C:\WINDOWS\3ystems2\apphieip.dif
C:\WINDOWS\AppPatch\sysmain.sdb
C:\WINDOWS\AppPatch\systest.sdb
  Opens:
  Opens:
                                     C:\WINDOWS\system32
  Opens:
  Opens:
                                     C:\WINDOWS\system32\cmd.exe.Manifest
C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
  Opens:
  Opens:
                                     C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
  Opens:
  Opens:
                                     C:\WINDOWS\AppPatch
  Opens
                                     C:\WINDOWS\system32\wbem
  Opens:
                                     C:\WINDOWS\WinSxS
                                         \WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
  Opens
Opens:
                                     C:\WINDOWS\system32\unicode.nls
C:\WINDOWS\system32\locale.nls
  Opens:
                                     C:\WINDOWS\system32\sorttbls.nls
C:\WINDOWS\system32\msvcrt.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\user32.dll
C:\WINDOWS\system32\gdi32.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\shimeng.dll
C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\advapi32.dll
C:\WINDOWS\system32\rpcrt4.dll
  Opens:
  Opens:
                                     C:\WINDOWS\system32\secur32.dll
C:\WINDOWS\system32\winmm.dll
  Opens:
  .
Opens
                                     C:\WINDOWS\system32\ole32.dll
C:\WINDOWS\system32\oleaut32.dll
  Opens:
  Opens:
  Opens:
                                     C:\WINDOWS\system32\msacm32.dll
C:\WINDOWS\system32\version.dll
  Opens:
                                     C:\WINDOWS\system32\shell32.dll
  Opens:
                                     C:\WINDOWS\system32\shlwapi.dll
                                     C:\WINDOWS\system32\userenv.dll
  Opens:
                                    C:\WINDOWS\system32\uxtheme.dll
C:\WINDOWS\system32\uxtheme.dll
C:\WINDOWS\system32\ctype.nls
C:\WINDOWS\system32\sortkey.nls
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
  Opens:
  Opens:
  Opens:
  Opens
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
                                    C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\wbm\wmic.exe
C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
  Opens:
  Opens:
  Opens:
  Opens
1003\$685c83111e534ea0f6bc8e25bc965f78\@
                                     C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens
                                     C:\WINDOWS\system32\SHELL32.dll.124.Config
C:\WINDOWS\WindowsShell.Config
C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:
  Opens:
  Opens:
                                     C:\WINDOWS\system32\comctl32.dll.124.Config
C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
  Opens:
  Opens:
                                     C:\WINDOWS\Temp\477ed5dc-1e37-4928-b33b-364159e99071
C:\WINDOWS\system32\calc.exe
  Opens:
  Opens:
                                     C:\WINDOWS\system32\drprov.dll
C:\WINDOWS\system32\ntlanman.dll
  Opens:
  Opens:
  Opens:
                                     C:\WINDOWS\system32\netui0.dll
C:\WINDOWS\system32\netui1.dll
  Opens:
                                     C:\WINDOWS\system32\netrap.dll
C:\WINDOWS\system32\samlib.dll
  Opens:
  Opens:
  Opens:
                                     C:\WINDOWS\system32\davclnt.dll
C:\WINDOWS\system32\MSIMTF.dll
                                     C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
  Writes to
1003\$685c83111e534ea0f6bc8e25bc965f78\@
  Writes to:
                                     C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
 1003\$685c83111e534ea0f6bc8e25bc965f78\n
                                    C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
  Writes to:
  Writes to:
                                     C:\WINDOWS\assembly\GAC\Desktop.ini
C:\WINDOWS\system32\rsaenh.dll
  Writes to:
  Reads from:
                                     C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
  Reads from:
                                     C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
                                     C:\WINDOWS\system32\calc.exe
  Reads from:
                                     C:\WINDOWS\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
  Deletes:
```

#### **Network Events**

DNS query:	j.maxmind.com
DNS response:	j.maxmind.com ⇒ 127.0.0.1
Connects to:	127.0.0.1:80
Sends data to:	8.8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	68.185.188.253:16471
Sends data to:	189.68.16.1:16471
Sends data to:	109.53.87.1:16471
Sends data to:	68.49.152.252:16471
Sends data to:	80.109.74.3:16471
Sends data to:	130.204.226.4:16471
Sends data to:	221.244.148.250:16471
Sends data to:	176.227.128.250:16471
Sends data to:	173.80.73.5:16471
Sends data to:	74.210.157.7:16471
Sends data to:	180.47.189.7:16471
Sends data to:	74.56.221.248:16471
Sends data to:	37.192.19.8:16471
Sends data to:	68.119.104.8:16471
Sends data to:	98.200.249.8:16471
Sends data to:	37.4.80.10:16471
Sends data to:	187.14.203.11:16471
Sends data to:	68.16.8.248:16471
Sends data to:	176.200.253.13:16471
Sends data to:	72.177.97.245:16471
Sends data to:	77.0.111.14:16471
Sends data to:	174.5.197.15:16471
Sends data to:	76.24.211.244:16471
Sends data to:	70.119.200.15:16471
Sends data to:	108.129.22.18:16471
Sends data to:	96.30.133.20:16471
Sends data to:	67.163.238.20:16471
Sends data to:	72.204.20.22:16471
Sends data to:	190.219.25.242:16471

```
Sends data to:
                              98.121.198.241:16471
                              200.127.18.241:16471
Sends data to:
Sends data to:
Sends data to:
                              217.209.199.22:16471
                              180.31.88.23:16471
Sends data to:
Sends data to
                              77.103.179.238:16471
146.247.84.238:16471
Sends data to:
Sends data to:
                              124.123.122.236:16471
69.204.104.236:16471
Sends data to:
Sends data to:
                              98.196.20.25:16471
                              109.192.63.25:16471
Sends data to:
                              151.43.129.233:16471
97.106.93.233:16471
Sends data to:
Sends data to:
Sends data to:
                              61.192.120.25:16471
Sends data to:
Sends data to:
                              75.74.160.229:16471
                              190.178.170.27:16471
95.223.50.224:16471
Sends data to:
Sends data to:
                               174.134.97.223:16471
Receives data from:
                              0.0.0.0:0
```

### Windows Registry Events

Creates key: HKCU\software\classes\clsid

HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9} Creates key:

Creates key: HKCl 409d6c4515e9}\inprocserver32 HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-

HKLM\software\clients\startmenuinternet Creates key:

Creates key: HKCR\http\shell

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

Creates key:  $\label{thm:limedia} \begin{tabular}{ll} HKCU \software \microsoft \multimedia \audio \ compression \ manager \mbox{$\backslash$ manager \mbox{$\backslash$$ HKCU\software\microsoft\multimedia\audio compression manager\priority Creates key:

v4.00

Creates key: HKCU\sessioninformation

Deletes value HKLM\software\microsoft\windows\currentversion\run[windows defender] Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\1be5bc13fd1cf615a95feec0c5b7fd13.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 kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll

Opens key: HKLM\software\microsoft\windows nt\currentversion\winlogon HKI M\

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

Opens key:  $\label{lem:hklm} \mbox{HKLM} \mbox{$\mbox{hklm}\software} \mbox{$\mbox{microsoft}\windows nt} \mbox{$\mbox{currentversion}\software} \mbox{$\mbox{$\mbox{microsoft}\software}\software} \mbox{$\mbox$ 

options\user32.dll

Opens key: HKLM\system\currentcontrolset\control\session manager Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key HKLM\software\policies\microsoft\windows\safer\codeidentifiers HKCU\software\policies\microsoft\windows\safer\codeidentifiers Opens key Opens key HKLM\software\microsoft\windows nt\currentversion\image file execution

options\imm32.dll

Opens kev: 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

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

options\gdi32.dll

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\shlwapi.dll Opens key:

HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument HKLM\software\microsoft\windows nt\currentversion\gre\_initialize Opens key HKLM\software\microsoft\windows nt\currentversion\compatibility32 HKLM\software\microsoft\windows nt\currentversion\ime compatibility Opens key: Opens key Opens key HKLM\software\microsoft\windows nt\currentversion\windows Opens key:  ${\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus performance}$ 

Opens key

Opens key: HKCU\software\policies\microsoft\control panel\desktop

Opens key HKCU\control panel\desktop

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

options\ole32.dll

Opens key: Opens key HKCR\interface

Opens key

HKCR\interface\{00020400-0000-0000-c000-000000000046} Opens key HKLM\software\microsoft\windows nt\currentversion\image file execution

options\cabinet.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\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000004

Opens key HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries

Opens key 

Opens key 

Opens key 

Opens key Opens key

Opens key 

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000

 $\label{thm:local_catalog} HKLM \system \current controlset \services \winsock 2 \parameters \protocol\_catalog \parameters \parameters \protocol\_catalog \parameters \p$ Opens key

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000010
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000011
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries
Opens key
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
  Opens kev:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
   Opens key:
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
                                                       HKLM\software\microsoft\rpc\pagedbuffers
   Opens key
                                                       HKLM\software\microsoft\runger
HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key
   Opens key
options\1be5bc13fd1cf615a95feec0c5b7fd13.exe\rpcthreadpoolthrottle
Openskey: HKLM\software\policies\microsoft\windows nt\rpc
   Opens key:
Opens key:
                                                       HKLM\software\microsoft\rpc\securityservice
HKLM\system\currentcontrolset\services\winsock\parameters
                                                       HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key:
   Opens key:
options\wshtcpip.dll
Opens key:
                                                       {\tt HKLM \backslash system \backslash current control \backslash computername}
   Opens key
                                                       \label{thm:loss} HKLM \system \current controls et \control \computer name \active computer name \hkLM \software \microsoft \cryptography \defaults \provider \microsoft \base
   Opens key
cryptographic provider v1.0
Opens key: HKI
                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
   Opens key:
                                                       HKLM\software\policies\microsoft\cryptography
   Opens key
                                                       HKLM\software\microsoft\cryptography
   Opens key
                                                       HKLM\software\microsoft\cryptography\offload
                                                       HKLM\software\microsoft\cryptography\deshashsessionkeybackward HKLM\software\microsoft\windows nt\currentversion\image file execution
   Opens key
   Opens key:
options\n
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc)
   Opens key:
HKLM \label{eq:hkklm} KLM \label{eq:hkklm} HKLM \label{eq:hkklm} Software \label{eq:hkklm} wire a year \label{eq:hkklm} Wilder \label{eq:hkklm} Wild
a949-c1b91af43b1a}
   Opens key:
                                                       HKLM\software\microsoft\windows\currentversion\run
   Opens key:
                                                       HKLM\software\microsoft\com3
                                                       HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
   Opens key
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
   Opens key:
   Opens key
                                                       HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0
00805fc1270e}\treatas
   Opens key:
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
    Opens key:
                                                       HKCU\software\classes
                                                       HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
   Opens key
00805fc1270e}\inprocserver32
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32
   Opens key:
Opens key: HKCU'
00805fc1270e}\inprocserverx86
                                                       HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
                                                       \label{local-hkcr-clsid-hkcr-clsid-hkcr-clsid-hkcu-software-classes-clsid-hkcu-software-classes-clsid-hkcu-software-classes-clsid-hkcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kcu-software-kc
  Opens key:
Opens key:
00805fc1270e}\localserver32
  Opens key:
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver32
   Opens key
                                                       HKCU \setminus software \setminus classes \setminus clsid \setminus \{ba126ae5-2166-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d1-b1d0-11d
00805fc1270e}\inprochandler32
   Opens key:
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32
   Opens key:
                                                       HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0
00805fc1270e}\inprochandlerx86
   Opens key:
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandlerx86
   Opens key
                                                       HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver
                                                       HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver
   Opens key:
                                                       HKCU\software\classes\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
   Opens key:
   Opens key
                                                       HKCU\software\classe\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
   Opens key
   Opens key
   Opens key
                                                       HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a
768597bd7223}\treatas
   Opens key:
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas
                                                       HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
   Opens key
768597bd7223}\inprocserver32
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32
   Opens key
   Opens key
                                                       HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a
768597bd7223}\inprocserverx86
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86
  Opens key:
                                                       HKCU\software\classes\clsid\{33c4643c-7811-46fa-
768597bd7223}\localserver32
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32
   Opens key:
                                                       HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a
   Opens key
768597bd7223}\inprochandler32
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32
  Opens key:
Opens key: HKCU\
768597bd7223}\inprochandlerx86
                                                       HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a
  Opens key:
Opens key:
                                                       768597bd7223}\localserver
   Opens key:
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver
   Opens key:
Opens key:
                                                       {\tt HKCU \ } software \ \\ classes \ \\ http
                                                       HKCR\http
  Opens key:
Opens key:
                                                       HKCU\software\classes\http\curver
                                                       HKCR\http\curver
   Opens key
                                                       HKCR\http\
   Opens key:
                                                       HKCU\software\classes\http\shell\open
   Opens key
                                                       HKCR\http\shell\open
   Opens key
                                                       HKCU\software\classes\http\shell\open\command
   Opens key
                                                       HKCR\http\shell\open\command
   Opens key:
                                                       HKCU\software\classes\http\shell
   Opens key
                                                       HKLM\software\classes
   Opens key
                                                       HKCR \verb|\clsid|{5839fca9-774d-42a1-acda-d6a79037f57f} \verb|\inprocserver32| \\
                                                       HKLM\system\currentcontrolset\enum\root\legacy_ntfs\0000
   Opens key
   Opens key
```

HKLM\system\currentcontrolset\enum\root\legacy ntfs\0000\root&legacy ntfs&0000

```
Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacv_null\0000
     Opens key
HKLM\svstem\currentcontrolset\enum\root\legacv null\0000\root&legacv null&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_partmgr\0000
    Opens key:
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_parvdm\0000
    Opens key:
Opens key: 
HKLM\system\currentcontrolset\enum\root\legacy_parvdm\0000\root&legacy_parvdm&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_policyagent\0000
    Opens key:
    Opens key:
Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_protectedstorage\0000
    Opens key
HKL\ M \ system \ current controls et \ legacy\_protected storage \ 0000 \ root \& legacy\_protected storage \& 0000 \ root \ Begacy\_protected storage \ which is the protected storage \ begacy\_protected storage \ begacy\_protected storage \ begacy\_protected \ storage \ begacy\_pro
    Opens kev:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_rasacd\0000
     Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rasacd\0000\root&legacy_rasacd&0000
    Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_rasman\0000
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_rasman\0000\root&legacy_rasman&0000
    Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy rdbss\0000
     Opens key
HKLM\system\currentcontrolset\enum\root\legacy_rdbss\0000\root&legacy_rdbss&0000
    Opens key:
Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_rdpcdd\0000
HKLMNsystem\currentcontrolset\enum\root\legacy_rdpcdd\0000\root&legacy_rdpcdd&0000
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_rdpp\0000
Opens key: 
HKLM\system\currentcontrolset\enum\root\legacy_rdpnp\0000\root&legacy_rdpnp&0000
    Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_rdpwd\0000
     Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_rdpwd\0000\root&legacy_rdpwd&0000

Opens key: HKLM\system\currentcontrolset\enum\root\legacy_remoteregistry\0000
    Opens key
\label{eq:hklm} \textbf{HKLM} \system \\ \textbf{currentcontrolset} \\ \textbf{enum} \\ \textbf{root} \\ \textbf{legacy\_remoteregistry} \\ \textbf{0000} \\ \textbf{root} \\ \textbf{2000} \\ \textbf{root} \\ \textbf{2000} \\ \textbf{root} \\ \textbf{2000} \\ 
    Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy rpcss\0000
HKLM\system\currentcontrolset\enum\root\legacy_rpcss\0000\root&legacy_rpcss&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_samss\0000
    Opens key:
    Opens key
HKLMNsystem\currentcontrolset\enum\root\legacy_samss\0000\root&legacy_samss&0000

Opens key: HKLM\system\currentcontrolset\enum\root\legacy_schedule\0000
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_schedule\0000\root&legacy_schedule&0000
    Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_seclogon\0000
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_seclogon\0000\root&legacy_seclogon&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_sens\0000
    Opens key:
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_sens\0000\root&legacy_sens&0000
   Opens kev:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_serial\0000
      Opens key
HKLM\system\currentcontrolset\enum\root\legacy serial\0000\root&legacy serial&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_sharedaccess\0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_shellhwdetection\0000
    Opens kev:
HKLM\system\currentcontrolset\enum\root\legacy shellhwdetection\0000\root&legacy shellhwdetection&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_snetmon\0000
    Opens key:
    Opens key
\label{thklm} HKLM\system \current control set \enum \cot \enum 
Opens key: HKLM\system\currentcontrolset\enum\root\legacy_spooler\0000\root&legacy_spooler&0000
    Opens key:
                                                                  HKLM\system\currentcontrolset\enum\root\legacy_sprocmon\0000
     Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_sprocmon\0000\root&legacy_sprocmon&0000 Opens key: HKLM\system\currentcontrolset\enum\root\legacy_sr\0000
    Opens key
\label{local-hklm} \begin{tabular}{ll} HKL\dot{M} & system \\ \cline{tabular} current control set \\ \cline{tabular} enum \\ \cline{tabular} root \\ \cline{tabular} enum \\ \cline{tabular} 
    Opens kev:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_sregmon\0000
    Opens key:
HKLM\system\currentcontrolset\enum\root\legacy sregmon\0000\root&legacy sregmon&0000
    Opens key:
    Opens key
Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy srservice\0000
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_srservice\0000\root&legacy_srservice&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_srv\0000
    Opens key:
    Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_srv\0000\root&legacy_srv&0000

Opens key: HKLM\system\currentcontrolset\enum\root\legacy_ssdpsrv\0000
    Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_ssdpsrv\0000\root&legacy_ssdpsrv&0000
   Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy stisvc\0000
      Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_tapisrv\0000
    Opens key:
    Opens key
Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_tcpip\0000
    Opens key:
HKLM\system\currentcontrolset\enum\root\legacy tcpip\0000\root&legacy tcpip&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_tdtcp\0000
    Opens key:
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_tdtcp\0000\root&legacy_tdtcp&0000

Opens key: HKLM\system\currentcontrolset\enum\root\legacy_termservice\0000
    Opens key
HKLM\system\currentcontrolset\enum\root\legacy_termservice\0000\root&legacy_termservice&0000
   Opens key:
Opens key:
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_themes\0000
HKLM\system\currentcontrolset\enum\root\legacy_themes\0000\root&legacy_themes&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_tlntsvr\0000
    Opens key:
    Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_tlntsvr\0000\root&legacy_tlntsvr&0000
   Opens kev:
                                                                  HKLM\system\currentcontrolset\enum\root\legacy_trkwks\0000
    Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_trkwks\0000\root&legacy_trkwks&0000
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_vga\0000
    Opens key
\label{local-hklm} \verb+KLM\system\currentcontrolset\enum\root\legacy\_vga\0000\root\&legacy\_vga\&0000\end{+}
                                                                   HKLM\system\currentcontrolset\enum\root\legacy_vgasave\0000
    Opens key:
```

```
HKLM\system\currentcontrolset\enum\root\legacy_vgasave\0000\root&legacy_vgasave&0000
     Opens kev:
                                                                                     HKLM\svstem\currentcontrolset\enum\root\legacv volsnap\0000
      Opens key
HKLM\system\currentcontrolset\enum\root\legacy volsnap\0000\root&legacy volsnap&0000
                                                                                     HKLM\system\currentcontrolset\enum\root\legacy_w32time\0000
      Opens key:
      Opens key
Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\legacy_wanarp\0000
      Opens key
HKLM\system\currentcontrolset\enum\root\legacy_wanarp\0000\root&legacy_wanarp&0000
     Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\legacy_webclient\0000
      Opens key:
HKLM\system\currentcontrolset\enum\root\legacy_webclient\0000\root&legacy_webclient&0000\root&legacy_webclient&0000\root\legacy_winmgmt\0000\root\legacy_winmgmt\0000\root\legacy_winmgmt\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\right\0000\ri
     Opens key
 HKLM\system\currentcontrolset\enum\root\legacy_winmgmt\0000\root&legacy_winmgmt&0000
     Opens key:
                                                                                     HKLM\system\currentcontrolset\enum\root\legacy wscsvc\0000
      Opens key:
                                                                                     HKLM\system\currentcontrolset\enum\root\legacy_wuauserv\0000
      Opens key
 HKLM\system\currentcontrolset\enum\root\legacy_wuauserv\0000\root&legacy_wuauserv&0000
     Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\legacy wzcsvc\0000
       Opens key
HKLM\system\currentcontrolset\enum\root\legacy_wzcsvc\0000\root&legacy_wzcsvc&0000
     Opens key:
Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\media\ms_mmacm
\label{local-problem} \parbox{$HKLM\system\currentcontrolset\enum\root\media\ms\_mmacm\root\media\ms\_mmacm\root\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmacm\media\ms\_mmac
                                                                                     HKLM\system\currentcontrolset\enum\root\media\ms_mmdrv
     Opens key
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_mmdrv\root&media&ms_mmdrv
     Opens key:
Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\media\ms_mmmci
HKLM\system\currentcontrolset\enum\root\media\ms_mmmci\root&media&ms_mmmci
Opens key: HKLM\system\currentcontrolset\enum\root\media\ms_i
                                                                                     HKLM\system\currentcontrolset\enum\root\media\ms_mmvcd
     Opens key
 HKLM\system\currentcontrolset\enum\root\media\ms_mmvcd\root&media&ms_mmvcd
     Opens key:
                                                                                     HKLM\system\currentcontrolset\enum\root\media\ms mmvid
      Opens key:
HKLM\system\currentcontrolset\enum\root\media\ms mmyid\root&media&ms mmyid
                                                                                     HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000
      Opens key:
      Opens key
\label{local-problem} \mbox{HKLM} \mbox{\current} controlset\mbox{\current} \mbox{\current} 
                                                                                    HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000
     Opens key:
      Opens key
HKLM\system\currentcontrolset\enum\root\ms ndiswanip\0000\root&ms ndiswanip&0000
     Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000
      Opens key:
HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000\root&ms_pppoeminiport&0000
                                                                                     HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000
     Opens key:
     Opens key
 HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000\root&ms_pptpminiport&0000
     Opens key:
                                                                                   HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0000
        Opens key
HKLM\system\currentcontrolset\enum\root\ms pschedmp\0000\root&ms pschedmp&0000
      Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001
      Opens key
 HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001\root&ms_pschedmp&0001
                                                                                    HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000
     Opens key:
Opens key:

HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000\root&ms_ptiminiport&0000
     Opens key:
Opens key:
                                                                                    HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000
HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000\root&nnetsec_mp&0000

Opens key: HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001
     Opens key
HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001\root&nnetsec_mp&0001
     Opens key:
                                                                                    \label{thm:loss} HKLM \system \current control set \enum \root \rdpdr \0000 \\ HKLM \system \current control set \enum \root \rdpdr \0000 \root \enum \root \rdpdr \0000 \\ \cot \enum \root \rdpdr \rdpdr \enum \root \rdpdr \rdpdr \rdpdr \enum \root \rdpdr \rdpdr
      Opens key:
     Opens key
                                                                                     HKLM\system\currentcontrolset\enum\root\rdp kbd\0000
                                                                                     HKLM\system\currentcontrolset\enum\root\rdp_kbd\0000\root&rdp_kbd&0000
      Opens key:
     Opens key
                                                                                     HKLM\system\currentcontrolset\enum\root\rdp mou\0000
      Opens key
                                                                                     Opens key
                                                                                     HKLM\system\currentcontrolset\enum\root\system\0000
      Opens key:
                                                                                     Opens key
                                                                                     HKLM\system\currentcontrolset\enum\root\system\0001
      Opens key
                                                                                     HKLM\system\currentcontrolset\enum\root\system\0001\root&system&0001
                                                                                     HKLM\system\currentcontrolset\enum\root\system\0002
      Opens key
      Opens key
                                                                                     HKLM\system\currentcontrolset\enum\root\system\0002\root&system&0002
      Opens key
Opens key
HKLM\system\currentcontrolset\enum\storage\volume\1&30a96598&0&signaturea045a045offset7e00length78aa94600\storage&volume&1&30a96598&0&signaturea045a045offset7e00length78aa94600
                                                                                     HKLM\system\currentcontrolset\enum\sw\{eeab7790-c514-11d1-b42b-
      Opens key
00805fc1270e}\asvncmac
                                                                                     HKLM \setminus system \setminus current control set \setminus enum \setminus sw \setminus \{eeab7790-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514-11d1-b42b-c514
      Opens key
00805fc1270e}\asyncmac\sw&{eeab7790-c514-11d1-b42b-00805fc1270e}&asyncmac
HKLM\svstem\currentcontrolset\enum\pci\ven 1022&dev 2000&subsys 20001022&rev 40\3&267a616a&0&18
      Opens key:
HKLM\system\currentcontrolset\enum\pci\ven 1022&dev 2000&subsys 20001022&rev 40\3&267a616a&0&18\pci&ven 1022&dev 2000&subsys 20001022&rev 40&3&267a616a&0&18
                                                                                    HKCU\software\policies\microsoft\windows\network connections HKLM\software\policies\microsoft\windows\network connections
      Opens key:
     Opens key:
Opens key:
08002b30309d}\shellfolder
                                                                                     HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-
     Opens key:
Opens key:
                                                                                   \label{lem:hkcr_lsid} HKCR\clsid_{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder \\ HKCU\software\microsoft\windows\currentversion\explorer\clsid_{2227a280-3ea-1069-a2de-08002b30309d}\shellfolder \\ HCU\software\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\microsoft\m
Jaea-1069-a2de-08002b30309d}
Openskey: HKCU\software\microsoft\windows\currentversion\policies\nonenum
     Opens key:
Opens key:
                                                                                     HKLM \verb|\software\microsoft\windows\currentversion\policies\nonenumerate that the limit of the 
a2de-08002b30309d}
Opens key: HKCU\software\m 3aea-1069-a2de-08002b30309d}\shellfolder
                                                                                     HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
     Opens key:
                                                                                    HKLM\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
 3aea-1069-a2de-08002b30309d}\shellfolder
                                                                                     HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
     Opens key:
      Opens key:
                                                                                     HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
                                                                                     HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\
      Opens key
                                                                                    HKCU\software\microsoft\windows\shellnoroam\muicache\
HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
      Opens key:
      Opens key
00805fc1270e}\shellfolder
```

HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder

Opens key:

Opens key

```
Opens key:
                                                                    HKLM\system\currentcontrolset\control\session manager\appcertdlls
     Opens key
                                                                    HKLM\system\currentcontrolset\control\session manager\appcompatibility
    Opens key
                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\apphelp.dll
    Opens key:
                                                                    HKLM\system\wpa\tabletpo
     Opens key:
                                                                    HKLM\system\wpa\mediacenter
                                                                    HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key
Opens key: HKCl
3202-11d1-aad2-00805fc1270e}
                                                                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
    Opens key:
                                                                    HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
    Opens key
                                                                    HKLM\software\microsoft\windows
\verb|nt\currentversion\appcompatflags\custom\cmd.exe|
    Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-
aad2-00805fc1270e}
Opens key: HKCU\software\m 3202-11d1-aad2-00805fc1270e}\shellfolder
                                                                   HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
                                                                   HKLM\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
    Opens key:
3202-11d1-aad2-00805fc1270e}\shellfolder
                                                                    HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
    Opens kev:
                                                                   HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\
     Opens key
    Opens key
                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\version.dll
    Opens key:
Opens key:
                                                                   HKLM\software\microsoft\windows nt\currentversion\appcompatflags HKCU\software\microsoft\windows nt\currentversion\appcompatflags
    Opens key
                                                                   HKLM\software\policies\microsoft\windows\safer\levelobjects
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
     Opens key
be2efd2c1a33}
     Opens key:
                                                                    HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-19
     Opens key
                                                                    HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
     Opens key:
edd5fbde1328}
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
    Opens key:
HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-1441-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-14411-1441-14411-14411-14411-14411-14411-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-1441-14
085bcc18a68d}
    Opens key:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
     Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens\ key: \\ HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens~key: \\ HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key: 
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: \label{local-bound} HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
    Opens kev:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
    Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
                                                                    HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
    Opens kev:
     Opens key:
                                                                    \label{local-observation} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalised \part \normalised \part \par
    Opens key
\label{local-observation} HKCU \software \policies \microsoft \windows \safer \code identifiers \normalised \nor
    Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
    Opens key
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
     Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key: \label{local-opens} HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key: \label{eq:hammon} \begin{tabular}{ll} & & \\ \begin{tabula
Opens key: 
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
    Opens key:
                                                                    HKCU\software\microsoft\windows\currentversion\explorer\shell folders
     Opens key
                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
     Opens key:
                                                                    HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.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

Opens key: options\oleaut32.dll

options\shimeng.dll
 Opens key:
options\winmm.dll

```
Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
   Opens kev:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\shell32.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
options\userenv.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
    Opens key:
 options\uxtheme.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\drivers32
    Opens key:
     Opens key:
Opens key:
                                                                  HKLM\software\microsoft\oleaut
                                                                  HKLM\software\microsoft\oleaut\userera
     Opens key:
     Opens key
                                                                  HKLM\software\microsoft\audiocompressionmanager\drivercache
     Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
     Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
     Opens key:
                                                                  HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
     Opens key
Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
     Opens key:
                                                                  HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
     Opens key
HKLM \label{limits} \begin{tabular}{ll} HKLM \label{limits} Software \end{tabular} in the constraint of the limits of the limi
     Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
                                                                  \label{thm:local} HKLM \software \microsoft \audiocompression manager \driver cache \mbox{\sc msacm.} 13 acm \\ HKLM \system \current control \sc \control \mbox{\sc mediare sources} \acm \\
     Opens key:
     Opens key:
    Opens key:
                                                                  HKLM\system\setup
     Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Openskey: HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
options\comctl32.dll
     Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\languagepack
     Opens key
     Opens key
                                                                  HKLM\system\currentcontrolset\control\productoptions
    Opens key:
                                                                  HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
    Opens key
                                                                  HKLM\software\policies\microsoft\windows\system
                                                                  HKCU\software\microsoft\windows\currentversion\themethkLM\system\currentcontrolset\services\sharedaccess
     Opens key
    Opens key
    Opens key:
                                                                  HKCU\software\classes\applications\calc.exe
                                                                  HKCR\applications\calc.exe
     Opens key
     Opens key:
                                                                  \label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\fileassociation \\ HKLM\software\microsoft\ctf\tip\end{kklm}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
    Opens key
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
    Opens key:
                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
 77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
    Opens key
                                                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
\label{lem:resolvent} $$7788731aa80} \add of the constraint of t
\label{eq:c9633771be64} $$ c9633771be64\\ \copens key: $$ HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-854c-46ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-86ed-4fcc-
Opens key: http://dae86bb7-262c-431e-9111-c974b6b7cac3}
Opens key: HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
77e8f3d1aa80}\categorv\item\{b5a73cd1-8355-426b-a161-259808f26b14}
                                                                  HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64\} \verb|\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04\}}|
Opens key: HKLM\software\microsoft\ctf\tip\{78cb5b0e 77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
                                                                  HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
    Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mpr.dll
     Opens key:
                                                                  {\tt HKLM \ } system \verb|\ current control \ $$ et \verb|\ control \ $$ hworder \ $$ hworder \ $$ et \ $$ hworder \ $$ hworder \ $$ has a substitution of the substitution o
     Opens key
                                                                  HKLM\svstem\currentcontrolset
     Opens key
                                                                  HKLM\system\currentcontrolset\services\rdpnp\networkprovider
                                                                  HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider
    Opens key
                                                                  HKLM\system\currentcontrolset\services\webclient\networkprovider
HKLM\software\microsoft\windows nt\currentversion\image file execution
     Opens key:
   Opens key:
options\drprov.dll
    Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netui0.dll
Opens key:
                                                                  HKLM\software\microsoft\windows nt\currentversion\network\world full
access shared parameters
    Opens key:
                                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
options\netrap.dll
Opens key:
options\samlib.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
Opens key:
options\netui1.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
Opens key:
options\ntlanman.dll
                                                                  HKLM\software\microsoft\windows nt\currentversion\image file execution
Opens key:
options\davclnt.dll
                                                                  \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ image file execution
   Opens key:
Opens key:
                                                                  HKCII\network
                                                                  HKCU\appevents\schemes\apps\.default\systemnotification\.current
    Queries value
Queries value
                                                                  HKLM\system\currentcontrolset\control\terminal server[tsappcompat] HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
                                                                  HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
     Queries value
     Queries value
     Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
    Oueries value:
                                                                  HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:
                                                                  HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[1be5bc13fd1cf615a95feec0c5b7fd13]
   Oueries value:
                                                                  HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[1be5bc13fd1cf615a95feec0c5b7fd13]
                                                                  HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls]
     Queries value:
     Queries value:
                                                                  {\tt HKCU \backslash control\ panel \backslash desktop[multiuilanguageid]}
                                                                  HKLM\system\currentcontrolset\control\session
    Queries value:
manager[criticalsectiontimeout]
                                                                  HKLM\software\microsoft\ole[rwlockresourcetimeout]
    Queries value:
```

```
Queries value:
                                                                                     HKCR\interface[interfacehelperdisableall]
                                                                                     HKCR\interface[interfacehelperdisableallforole32]
     Oueries value:
                                                                                     HKCR\interface[interfacehelperdisabletvpelib]
     Oueries value
                                                                                     HKCR\interface\{00020400-0000-0000-c000-
00000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-00000000000046}[interfacehelperdisableallforole32]
     Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock registry version]
     Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
     Queries value
Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[num catalog entries]
     Oueries value:
Queries value
Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000003[packedcatalogitem]
     Queries value
Oueries value:
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \code 000000000005 \cite{thmose} \parameters \protocol\_catalog9 \cite{thmose} \parameters \parameters \protocol\_catalog9 \cite{thmose} \parameters \pa
     Queries value
HKLM \system \current controls et \services \winsock 2 \parameters \protocol\_catalog \parameter \
     Oueries value
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000011[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5[serial access num]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5[num catalog entries]
HKL\\ M\system\current controlset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog\_entries\space\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\catalog3\c
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000001[displaystring]
     Queries value:
\label{thm:hklm:hkl} \begin{tabular}{ll} HKL\begin{tabular}{ll} MKL\begin{tabular}{ll} MK
     Oueries value:
Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000001[enabled]
     Queries value
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001 \ [version]
     Oueries value:
Queries value
HKL\\ M\system\current control set\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
     Oueries value
HKLM \system \verb| current control set \verb| services | winsock \verb| 2 parameters \verb| namespace_catalog \verb| S catalog_entries | winsock \verb| 2 parameters | wi
     Queries value:
HKLM \system \verb|\currentcontrolset| services \verb|\winsock2| parameters \verb|\namespace_catalog5| catalog_entries \verb|\currentcontrolset| services \swinsock2| parameters \verb|\namespace_catalog5| catalog_entries \swinsock2| parameters \swi
     Oueries value
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[enabled]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000002[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003flibrarypath]
     Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\000000000003[displaystring]
HKL\ Mksystem \ (current controls et \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ (catalog\_entries \ 0000000000003 [providerid]) \ (catalog\_entries \ namespace\_catalog 5) \ (catalog
     Queries value
Oueries value
Oueries value
Oueries value
\label{thm:mass} HKL \begin{tabular}{ll} MKL \begin{
     Oueries value
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5\catalog entries\00000000003[storesserviceclassinfo]
     Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
     Queries value:
\label{local-hklm} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ All $$ is a simple of the control of the c
                                                                                     HKLM\software\microsoft\rpc[maxrpcsize]
     Queries value:
                                                                                    HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
HKLM\system\currentcontrolset\services\winsock\parameters[transports]
     Oueries value:
     Queries value:
     Queries value:
                                                                                     HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [mapping]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
     Queries value
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
                                                                                     HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
                                                                                    HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
                                                                                    HKLM\system\currentcontrolset\control\session
     Queries value
```

manager[safeprocesssearchmode]

```
\label{thm:local_hammon_hammon} HKLM\software\mbox{\sc microsoft\com3[regdbversion]}
       Queries value
                                                                                             HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid]
      Oueries value:
                                                                                            HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[dllsurrogate]
HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[localservice]
      Queries value
      Queries value:
Queries value: HKCR\clsid\{33c4643r768597bd7223}\inprocserver32[inprocserver32]
                                                                                             HKCR\clsid\{33c4643c-7811-46fa-a89a-
      Queries value
                                                                                            HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[appid]
      Queries value:
                                                                                            HKCR\http\shell\open\command[]
HKLM\software\clients\startmenuinternet[]
      Queries value:
      Queries value:
                                                                                             Oueries value
      Queries value
      Queries value:
                                                                                             HKLM \verb|\system| current controlset \verb|\enum| root \verb|\legacy_parvdm| 0000 [class guid]
                                                                                             HKLM\system\currentcontrolset\enum\root\legacy_rasacd\0000[classguid]
      Queries value
                                                                                            \label{thm:loss} HKLM \system \current controls et \enum \cot \legacy\_rdpcdd \coto \cite{thm:loss} id] HKLM \system \current \cot \cite{thm:loss} et \cite{thm:loss
      Oueries value:
      Queries value
                                                                                            \label{thm:loss} HKLM \system \current control set \enum \root \legacy\_serial \current control set \enum \root \legacy\_snet \enum \root \legacy\_snet \enum \root \legacy\_snet \enum \root \legacy\_snet \enum \root \ro
      Queries value:
      Queries value:
                                                                                           HKLM\system\currentcontrolset\enum\root\legacy_srecimon\0000[classguid]
HKLM\system\currentcontrolset\enum\root\legacy_srpcomon\0000[classguid]
HKLM\system\currentcontrolset\enum\root\legacy_sregmon\0000[classguid]
HKLM\system\currentcontrolset\enum\root\legacy_sroot\bigoup\0000[classguid]
HKLM\system\currentcontrolset\enum\root\legacy_tcpip\0000[classguid]
      Oueries value:
      Queries value
      Queries value:
      Queries value
      Queries value
                                                                                             \label{thm:loss} HKLM\system\currentcontrolset\enum\root\legacy\_vgasave\0000[classguid] HKLM\system\currentcontrolset\enum\root\legacy\_volsnap\0000[classguid] \\
      Queries value
      Queries value:
      Queries value
                                                                                            \label{lem:hklm} HKLM \end{substitute} HKLM \end{substitute} HKLM \end{substitute} Note that the substitute of the sub
      Queries value
                                                                                            \label{thm:loss} HKLM \system \current controls et \enum \root \media \mbox{\tt mmdrv} [class guid] \\ HKLM \system \current controls et \enum \root \mbox{\tt media} \mbox{\tt mmci} [class guid] \\
      Queries value:
      Queries value:
                                                                                            Queries value
      Queries value
                                                                                            \label{thm:loss} HKLM\system\currentcontrolset\enum\root\ms_12tpminiport\0000[classguid] \\ HKLM\system\currentcontrolset\enum\root\ms_ndiswanip\0000[classguid] \\
      Queries value:
      Queries value
      Oueries value:
                                                                                             HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[classguid]
                                                                                             HKLM\system\currentcontrolset\enum\root\ms_pptpminiport\0000[classguid]
      Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
     Oueries value:
                                                                                             HKLM\system\currentcontrolset\enum\root\ms pschedmp\0000[classguid]
      Queries value
                                                                                             HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001[classguid]
      Queries value:
                                                                                             HKLM\system\currentcontrolset\enum\root\ms ptiminiport\0000[classguid]
                                                                                            HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0000[classguid] HKLM\system\currentcontrolset\enum\root\nnetsec_mp\00001[classguid]
      Queries value:
     Queries value:
                                                                                            HKLM\system\currentcontrolset\enum\root\rdpdr\000[classguid] HKLM\system\currentcontrolset\enum\root\rdp_kbd\0000[classguid]
      Oueries value:
      Queries value:
      Queries value:
                                                                                            HKLM\system\currentcontrolset\enum\root\rdp_mou\0000[classguid]
HKLM\system\currentcontrolset\enum\root\system\0000[classguid]
      Queries value:
      Oueries value:
                                                                                             HKLM\system\currentcontrolset\enum\root\system\0001[classguid]
      Queries value
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]

Queries value: HKLM\system\currentcontrolset\enum\root\system\0002[classguid]
     Oueries value
HKLM\system\current controls et\enum\storage\volume\1\&30a96598\&0\&signaturea045a045offs et7e00length 78aa94600\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\classguid\clas
     Queries value
HKLM\system\currentcontrolset\enum\pci\ven_1022&dev_2000&subsys_20001022&rev_40\3&267a616a&0&18[driver]
      Oueries value
HKL\\ M\system\currentcontrolset\enum\pci\ven\_1022\&dev\_2000\&subsys\_20001022\&rev\_40\3\&267a616a\&0\&18[capabilities]
      Queries value
HKL \\ MN system \\ current control set \\ enum \\ pci \\ ven\_1022 \\ dev\_2000 \\ &subsys\_20001022 \\ &rev\_40 \\ \\ &3267 \\ a616 \\ a60 \\ &818 \\ [configflags]
      Oueries value
Queries value:
\label{thk_mass} \begin{tabular}{ll} HKLM\system\currentcontrolset\enum\pci\ven\_1022\&dev\_2000\&subsys\_20001022\&rev\_40\3\&267a616a\&0\&18[friendlyname] \\ Queries value: \end{tabular}
\label{local-prop} HKLM\system\currentcontrolset\enum\proi\ven_1022\&dev_2000\&subsys_20001022\&rev_40\as267a616a\&0\&18[devicedesc]\\ Queries\value: HKLM\system\currentcontrolset\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\mbox{$m$$\currentcontrolset}\enum\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit\proit
      Oueries value:
                                                                                             HKLM\svstem\currentcontrolset\enum\root\ms ndiswanip\0000[driver]
      Queries value
                                                                                             HKLM\system\currentcontrolset\enum\root\ms_pppoeminiport\0000[driver]
                                                                                            \label{local-hklm-system-current} HKLM\system\currentcontrolset\enum\root\mbox{\sc m_pptpminiport}\0000[driver] \\ HKLM\system\currentcontrolset\enum\root\mbox{\sc m_pschedmp}\0000[driver] \\
     Queries value:
      Queries value
      Oueries value:
                                                                                             HKLM\system\currentcontrolset\enum\root\ms_pschedmp\0001[driver]
      Queries value
                                                                                             HKLM\system\currentcontrolset\enum\root\ms_ptiminiport\0000[driver]
      Queries value:
                                                                                             HKLM\system\currentcontrolset\enum\root\nnetsec mp\0000[driver]
                                                                                            HKLM\system\currentcontrolset\enum\root\nnetsec_mp\0001[driver]
HKCR\clsid\{2227a280-3aea-1069-a2de-
      Queries value
      Oueries value:
08002b30309d}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[attributes]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[callforattributes]
     Queries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{2227a280-3aea-1069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de-4069-a2de
08002b30309d}]
     Oueries value
                                                                                             HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[hidefolderverbs]
                                                                                             HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
     Queries value:
       Queries value
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll.-9319]
                                                                                             HKLM\system\currentcontrolset\control\session
     Queries value:
00805fc1270e}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[attributes]
      Queries value:
\label{thm:local_ham} \begin{tabular}{ll} HKLM \label{thm:local_ham} HKLM \label{thm:local_ham} \begin{tabular}{ll} H
00805fc1270e}]
     Queries value
                                                                                             HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[hidefolderverbs]
      Queries value
                                                                                            HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\netshell.dll.-1200]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
      Queries value
                                                                                             HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
     Oueries value:
                                                                                             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
19[refcount]
     Queries value:
be2efd2c1a33}[itemdata]
```

Queries value:

```
be2efd2c1a33}[saferflags]
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
    Queries value:
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \software \policies \microsoft \windows \safer \code identifiers \norm{1}{0} \hashes \code identifiers \norm{1}{0} \hashes \code identifiers \norm{1}{0} \hashes \norm{
edd5fbde1328}[hashalg]
    Oueries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\f7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
     Queries value
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}[hashalg]
     Oueries value:
HKLM \setminus Software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 0 \setminus hashes \setminus \{7fb9cd2e-3076-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57b-4df9-a57
b813f72dbb91}[itemsize]
     Queries value
b813f72dbb91}[saferflags]
     Queries value:
7c29ddecae3f}[itemdata]
Queries\ value: \\ HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d-4762-b16d
7c29ddecae3f}[hashalg]
     Queries value:
7c29ddecae3f}[itemsize]
    Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
     Queries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
     Queries value:
HKLM \software \policies \microsoft \windows \safer \code identifiers \noindent \noi
     Queries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
    Queries value:
085bcc18a68d}[saferflags]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
     Queries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
    Oueries value:
b91490411bfc}[itemsize]
b91490411bfc}[saferflags]
     Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
     Queries value
\label{local_HKLM} \begin{tabular}{ll} HKLM \software \policies \microsoft \windows \safer \code identifiers [policy scope] \\ Queries value: HKCU \software \microsoft \windows \current version \explorer \shell \\ \end{tabular}
     Queries value
folders[cache]
     Queries value
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
     Queries value:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
                                                                                 HKLM\software\microsoft\windows nt\currentversion\ime compatibilitv[cmd]
     Oueries value:
     Queries value
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
    Queries value:
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
     Queries value:
     Oueries value:
     Queries value
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
     Queries value:
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
     Queries value:
     Queries value:
     Queries value
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
     Queries value
     Queries value:
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
     Queries value:
     Oueries value:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
     Queries value
     Queries 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]
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
     Queries value
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
     Queries value:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
     Queries value:
     Queries value
     Queries value
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
     Queries value:
     Queries value:
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
     Queries value:
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
     Queries value:
     Queries value
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
     Queries value
     Queries value
     Queries value:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
     Queries value
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
     Queries value:
                                                                                \label{thm:local-hklm} HKLM \software \microsoft \windows nt \current version \drivers 32 \mbox{[mixer1]} \\ HKLM \software \mbox{\software} 
     Queries value:
     Queries value
    Oueries value:
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
     Oueries value
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
     Queries value:
     Queries value:
     Queries value:
     Oueries value
                                                                                 HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
```

HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]

Queries value:

```
Queries value:
                                                                                                                                                                HKCU\software\microsoft\multimedia\audio[systemformats]
           Queries value
                                                                                                                                                                HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
           Oueries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
\label{thm:local_manager} \begin{tabular}{ll} HKLM \lab
           Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
           Queries value:
\label{thm:local_manager} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} and $$ positive reache \end{tabular} $$ im a adpcm [cfilter tags] $$ im a constant $$ positive reache \end{tabular} $$ positive reache \end{tabular} $$ im a constant $$ positive reache \end{tabular} $$ positive reacher \end{tab
         Queries value
                                                                                                                                                                HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
         Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
         Oueries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a compression manager \label{lem:hklm} which is a compression manager \label{lem:hklm}. The compression manager \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Which is a compression manager \label{lem:hklm}. The compression manager \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Which is a compression manager \label{lem:hklm}. The compression manager \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Which is a compression manager \label{lem:hklm}. The compression manager \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Which is a compression manager \label{lem:hklm} \label{lklm} \lab
       Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
           Oueries value:
\label{thm:hammon} HKLM\software\mbox{\tt hm:crosoft\audiocompressionmanager\drivercache\mbox{\tt hm:msadpcm[cfiltertags]}} \\ Queries\value: HKLM\software\mbox{\tt hm:crosoft\ware\mbox{\tt hm:msadpcm[cfiltertags]}} \\
nt\currentversion\drivers32[msacm.msg711]
         Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} with a compression manager \label{lem:hklm} driver cache \label{lem:hklm} \label{lem:hklm} with a compression manager \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} 
         Queries value:
\label{thm:local_hammager} \textbf{HKLM} \\ \textbf{Software} \\ \textbf{microsoft} \\ \textbf{audiocompression} \\ \textbf{manager} \\ \textbf{drivercache} \\ \textbf{msacm.msg711[cformattags]} \\ \textbf{ms
           Oueries value
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} icrosoft \label{lem:hklm} adjacent \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} \label{lklm} \label{
           Queries value:
\label{localization} HH\dot{L}M\software\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\mbox{\compressionmanager\drivercache\drivercache\mbox{\compressionmanager\drivercache\drivercache\drivercache\drivercache\drivercache\drivercache\drivercache\drivercache\drivercache\drivercache
nt\currentversion\drivers32[msacm.msgsm610]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610\Gaformattagcachel
           Queries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
Queries value: HKLM\software\mi nt\currentversion\drivers32[msacm.trspch]
                                                                                                                                                              HKLM\software\microsoft\windows
           Queries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
           Queries value
\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} $$ in manager \end{tabular
         Oueries value:
\label{thm:local_hamma} \begin{tabular}{ll} HKLM \end{tabular} software \verb|\microsoft| audiocompression manager \end{tabular} driver cache \end{tabular} mattag cache] $$ \end{tabular} $$ \begin{tabular}{ll} HKLM \end{tabular} $$ \begin{tab
         Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
       Oueries value:
                                                                                                                                                             HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
         Queries value:
Oueries value:
Queries value:
\label{thm:mass} \begin{tabular}{ll} HKLM \end{tabular} \begin{tabular}{ll} HKLM \end{tabular} software \end{tabular} icrosoft \end{tabular} audio compression manager \end{tabular} \begin{tabular}{ll} driver cache \end{tabular} msg723 [a formattag cache] \end{tabular}
         Queries value:
\label{local_HKLM} HKLM \software \ensuremath{\mbox{\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$}\mbox{$\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mbox{$}\mb
nt\currentversion\drivers32[msacm.msaudio1]
           Oueries value
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} which is a constraint of the lemma of the lemm
           Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
           Queries value:
                                                                                                                                                              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[fdwsupport]
           Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl anet[cformattags]
           Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
           Queries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
         Queries value:
                                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
           Oueries value
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
           Queries value
HKLM \label{limits} No ftware \mbox{$\mbox{$\mbox{$m$} incosoft$} audio compression manager \mbox{$\mbox{$\mbox{$d$} incos
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
           Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
                                                                                                                                                                HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.13acm]
           Queries value:
           Queries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} Software \mbox{$\mathbb{N}$ in the last of th
         Queries value:
\label{thm:local} \begin{tabular}{ll} HKLM \label{thm:local} Software \end{tabular} in the local discontinuous constraints of the loc
           Oueries value:
HKLM \label{lem:hklm} \label{lem:hklm} HKLM \label{lem:hklm} I3acm [a formattag cache] \\
           Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
           Queries value:
                                                                                                                                                                \label{thm:limedia} \mbox{HKCU\software\mbox{\sc microsoft\mbox{\sc multimedia}\audio\ compression\ manager\sc priority} }
v4.00[priority1]
           Queries value
                                                                                                                                                                {\tt HKLM \backslash system \backslash setup[system setup in progress]}
           Queries value:
                                                                                                                                                                HKCU\control panel\desktop[smoothscroll]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
           Oueries value:
                                                                                                                                                              HKLM\software\microsoft\window
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]
                                                    HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
    Queries value
                                                    HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
    Queries value:
                                                    HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
    Queries value:
    Oueries value
                                                    HKCU\control panel\desktop[lamebuttontext]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\sharedaccess[start]
    Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
   Queries value
\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \end{tabular} Software \end{tabular} in \begin{tabular}{ll} cutlist \end{tabular} I \begin{tabu
   Queries value
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
   Oueries value
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Queries value:
77e8f3d1aa80\} \\ category \\ item \\ \{5130a009-5540-4fcf-97eb-aad33fc0ee09\} \\ [dword]
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
   Oueries value:
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
   Queries value:
                                                    HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80\} \land [dword]
   Queries value:
HKLM\system\currentcontrolset\control\networkprovider\hworder[providerorder]

Queries value: HKLM\system\currentcontrolset\services\rdpn\networkprovider[name]
    Oueries value:
                                                    Queries value:
HKLM\system\currentcontrolset\services\rdpnp\networkprovider[providerpath]
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[name]
HKLM\svstem\currentcontrolset\services\lanmanworkstation\networkprovider[class]
HKLM\system\currentcontrolset\services\lanmanworkstation\networkprovider[providerpath]
    Queries value:
                                                    HKLM\system\currentcontrolset\services\webclient\networkprovider[name]
    Oueries value:
                                                    HKLM\system\currentcontrolset\services\webclient\networkprovider[class]
    Oueries value:
HKLM\system\currentcontrolset\services\webclient\networkprovider[providerpath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\network\world full access shared parameters[sort hyphens]
                                                    HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
   Oueries value:
    Sets/Creates value:
409d6c4515e9}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[]
    Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exel
                                                    HKLM\software\microsoft\cryptograph\rng[seed]
HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
    Value changes:
    Value changes:
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog \quad \entries \colong 000000000011 \packed catalog item]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000000fpackedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
    Value changes
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
    Value changes
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \colonormal times \parameter \paramete
   Value changes
HKLM \system \current control set \services \winsock 2 \parameters \protocol\_catalog9 \catalog\_entries \code 000000000001 \[packed catalog item] \end{subarray} \label{lem:lem:hklm}
```

 $HKLM \system \current controls et\services \winsock 2\parameters \names pace\_catalog 5 \catalog\_entries \names \names pace\_catalog 5 \catalog\_entries \names \na$ 

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \namespace\_catal$ 

HKCU\sessioninformation[programcount]

Value changes:

Value changes:

Value changes: