# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3312, Task ID: 756

Task ID: 756 Risk Level: 10

Date Processed: 2016-05-18 10:34:15 (UTC)

Processing Time: 62.2 seconds IntelliVM Virtual Environment:

**Execution Arguments:** "c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"

Sample ID: Type: basic admin Owner:

859ba9477553ccad1bba34c555ab6a1b Label:

Date Added: 2016-05-18 10:30:49 (UTC) File Type: PE32:win32:gui

File Size: 199680 bytes

859ba9477553ccad1bba34c555ab6a1b MD5:

339ff6766efd4c5f26a8c0c9413b68ae664bb5eb8dfa403bec5df2909cbb73a1 SHA256:

Description: None

# Pattern Matching Results

Modifies registry autorun entries

- Writes to memory of system processes
- 3 HTTP connection response code 200 (success)
- PE: Nonstandard section 5 Abnormal sleep detected
- 5 Installs service
- Creates file in recycle bin
- Changes Winsock providers
- 10 Creates malicious events: ZeroAccess [Rootkit]
- 4 Reads process memory
- 5 PE: Contains compressed section
- 7 Creates threads in system processes
- Opens a recycle bin location
- 3 Long sleep detected
- 7 Injects thread into Windows process

### Static Events

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

### Process/Thread Events

Creates process: C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

["c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe" ]

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

Reads from process: PID:1728 C:\WINDOWS\system32\calc.exe PID:1904 C:\WINDOWS\explorer.exe Writes to process: Writes to process: PID:896 C:\WINDOWS\system32\services.exe Writes to process: PID:576 C:\WINDOWS\system32\cmd.exe

Terminates process: C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

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

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

# Named Object Events

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

\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1} Creates event: Creates event: \BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78} \BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77} Creates event:

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

\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000007B8.00000000.00000004

\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000007B8.00000000.00000004 Creates event:

Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.ILH.IC

Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.ILH.IC 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

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

1003\\$685c83111e534ea0f6bc8e25bc965f78

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

1003\\$685c83111e534ea0f6bc8e25bc965f78\L

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

```
1003\$685c83111e534ea0f6bc8e25bc965f78\U
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
 Creates:
1003\$685c83111e534ea0f6bc8e25bc965f78\@
 Creates:
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\n
 Creates:
                         C:\RECYCLER\
 Creates:
                         C:\RECYCLER\S-1-5-18
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
 Creates:
 Creates:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\L
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
 Creates:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
 Creates:
 Creates:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
 Creates:
                         C:GAC MSIL
                         C:\WINDOWS\assembly\GAC
 Creates:
 Creates:
                         C:\WINDOWS\assembly\GAC\Desktop.ini
                         C:\WINDOWS\Prefetch\859BA9477553CCAD1BBA34C555AB6-0659C491.pf
 Opens:
                         C:\Documents and Settings\Admin
 Opens:
 Opens:
                         C:\WINDOWS\system32\atl.dll
 Opens:
                         C:\WINDOWS\system32\imm32.dll
                         C:\WINDOWS\system32\cabinet.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\ws2_32.dll
 Opens:
                         C:\WINDOWS\system32\ws2help.dll
 Opens:
                         C:\WINDOWS\system32\mswsock.dll
 Opens:
                         C:\WINDOWS\system32\hnetcfg.dll
 Opens:
                         C:\WINDOWS\system32\wshtcpip.dll
 Opens:
                         C:\WINDOWS\system32\rsaenh.dll
 Opens:
                         C:\WINDOWS\system32\crypt32.dll
 Opens:
                         C:\WINDOWS
 Opens:
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78
 Opens:
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
1003\$685c83111e534ea0f6bc8e25bc965f78\n
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78
 Opens:
 Opens:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\n
 Opens:
                         C:\WINDOWS\assemblv
 Opens:
                         C:\WINDOWS\system32\cmd.exe
 Opens:
                         C:\WINDOWS\system32\apphelp.dll
 Opens:
                         C:\WINDOWS\AppPatch\sysmain.sdb
 Opens:
                         C:\WINDOWS\AppPatch\systest.sdb
 Opens:
                         C:\WINDOWS\system32
                         C:\
 Opens:
 Opens:
                         C:\WINDOWS\assembly\GAC\Desktop.ini
 Opens:
                         C:\WINDOWS\assembly\GAC
                         C:\WINDOWS\system32\cmd.exe.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
 Opens:
                         C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf
 Opens:
                         C:
 Opens:
                         C:\WINDOWS\AppPatch
                         C:\WINDOWS\system32\wbem
 Opens:
                         C:\WINDOWS\WinSxS
 Opens:
 Opens:
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls 6595b64144ccf1df 6.0.2600.5512 x-ww 35d4ce83
 Opens:
                         C:\WINDOWS\system32\ntdll.dll
 Opens:
                         C:\WINDOWS\system32\kernel32.dll
 Opens:
                         C:\WINDOWS\system32\unicode.nls
 Opens:
                         C:\WINDOWS\system32\locale.nls
 Opens:
                         C:\WINDOWS\system32\sorttbls.nls
 Opens:
                         C:\WINDOWS\system32\msvcrt.dll
 Opens:
                         C:\WINDOWS\system32\user32.dll
 Opens:
                         C:\WINDOWS\system32\gdi32.dll
 Opens:
                         C:\WINDOWS\system32\shimeng.dll
 Opens:
                         C:\WINDOWS\AppPatch\AcGenral.dll
 Opens:
                         C:\WINDOWS\system32\advapi32.dll
 Opens:
                         C:\WINDOWS\system32\rpcrt4.dll
 Opens:
                         C:\WINDOWS\system32\secur32.dll
 Opens:
                         C:\WINDOWS\system32\winmm.dll
 Opens:
                         C:\WINDOWS\system32\ole32.dll
 Opens:
                         C:\WINDOWS\system32\oleaut32.dll
 Opens:
                         C:\WINDOWS\system32\msacm32.dll
 Opens:
                         C:\WINDOWS\system32\version.dll
                         C:\WINDOWS\system32\shell32.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\shlwapi.dll
                         C:\WINDOWS\system32\userenv.dll
 Opens:
 Opens:
                         C:\WINDOWS\system32\uxtheme.dll
 Opens:
                         C:\WINDOWS\system32\ctype.nls
 Opens:
                         C:\WINDOWS\svstem32\sortkev.nls
                         C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
 Opens:
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
 Opens:
                         C:\WINDOWS\WindowsShell.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll
 Opens:
                         C:\WINDOWS\system32\wbem\wmic.exe
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\@
 Opens:
 Opens:
                         C:\RECYCLER\S-1-5-21-1757981266-507921405-1957994488-
```

```
1003\$685c83111e534ea0f6bc8e25bc965f78\@
                        C:\WINDOWS\system32\SHELL32.dll.124.Manifest
 Opens:
 Opens:
                         C:\WINDOWS\system32\SHELL32.dll.124.Config
 Opens:
                         C:\WINDOWS\WindowsShell.Config
 Opens:
                        C:\WINDOWS\system32\comctl32.dll.124.Manifest
 Opens:
                         C:\WINDOWS\system32\comctl32.dll.124.Config
 Opens:
                         C:\RECYCLER\S-1-5-18\$685c83111e534ea0f6bc8e25bc965f78\U
                         C:\WINDOWS\Temp\100727f2-bbf4-4b86-92ba-5c99b64f3982
 Opens:
                         C:\WINDOWS\system32\calc.exe
 Opens:
 Opens:
                         C:\WINDOWS\system32\MSIMTF.dll
```

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

1003\\$685c83111e534ea0f6bc8e25bc965f78\@

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

1003\\$685c83111e534ea0f6bc8e25bc965f78\n

C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\@ Writes to: Writes to: C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\n

Writes to: C:\WINDOWS\assembly\GAC\Desktop.ini C:\WINDOWS\system32\rsaenh.dll Reads from: Reads from: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

C:\RECYCLER\S-1-5-18\\$685c83111e534ea0f6bc8e25bc965f78\@ Reads from:

Reads from: C:\WINDOWS\system32\calc.exe

Deletes: C:\WINDOWS\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Network Events	
DNS query:	promos.fling.com
DNS response:	promos.fling.com ⇒ 208.91.207.58
Connects to:	208.91.207.58:80
Connects to:	213.108.252.185:80
Sends data to:	8.8.8.8:53
Sends data to:	promos.fling.com:80 (208.91.207.58)
Sends data to:	213.108.252.185:80
Sends data to:	83.133.123.20:53
Sends data to:	37.112.0.251:16471
Sends data to:	68.104.123.244:16471
Sends data to:	99.225.75.244:16471
Sends data to:	94.240.212.241:16471
Sends data to:	111.65.195.241:16471
Sends data to:	184.66.166.241:16471
Sends data to:	74.129.114.241:16471
Sends data to:	70.176.247.237:16471
Sends data to:	125.4.212.237:16471
Sends data to:	94.24.192.232:16471
Sends data to:	182.1.253.230:16471
Sends data to:	87.3.88.229:16471
Sends data to:	210.2.239.226:16471
Sends data to:	71.62.37.224:16471
Sends data to:	66.158.225.2:16471
Sends data to:	69.242.115.222:16471
Sends data to:	178.48.109.222:16471
Sends data to:	83.14.18.222:16471
Sends data to:	90.229.137.221:16471
Sends data to:	219.173.240.2:16471
Sends data to:	115.38.18.4:16471
Sends data to:	72.48.52.8:16471
Sends data to:	68.148.21.218:16471
Sends data to:	46.237.125.216:16471
Sends data to:	98.220.121.216:16471
Sends data to:	89.214.82.216:16471
Sends data to:	85.230.116.8:16471
Sends data to:	173.19.154.215:16471
Sends data to:	206.53.110.9:16471
Sends data to:	142.167.122.9:16471
Sends data to:	89.132.206.9:16471
Sends data to:	75.131.172.213:16471
Sends data to:	78.23.0.213:16471
Sends data to:	186.10.14.10:16471
Sends data to:	76.123.75.212:16471
Sends data to:	113.211.35.11:16471
Sends data to:	122.31.235.211:16471
Sends data to:	46.128.24.13:16471
Sends data to:	114.74.200.13:16471
Sends data to:	87.1.83.15:16471
Sends data to:	138.124.19.16:16471
Sends data to:	121.84.80.16:16471
Sends data to:	76.126.235.205:16471
Sends data to:	69.143.155.205:16471
Sends data to:	151.33.20.205:16471
Sends data to:	93.171.119.17:16471
Sends data to:	89.181.132.204:16471
Sends data to:	24.222.98.204:16471
Sends data to:	94.19.131.17:16471
Sends data to:	65.31.38.203:16471

Receives data from: 0.0.0.0:0

Receives data from: promos.fling.com:80 (208.91.207.58)

Receives data from: 213.108.252.185:80

# Windows Registry Events

Creates key: HKCU\software\classes\clsid

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

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

409d6c4515e9}\inprocserver32

Creates key: HKLM\software\clients\startmenuinternet

Creates key: HKCR\http\shell

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

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

v4.00

Creates key: HKCU\sessioninformation

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

options\859ba9477553ccad1bba34c555ab6a1b.exe

Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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

options\gdi32.dll

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

options\user32.dll

Opens kev: HKLM\system\currentcontrol\set\control\session manager

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

options\imm32.dll

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

options\ntdll.dll

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

options\kernel32.dll

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

options\msvcrt.dll

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

options\atl.dll

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

options\secur32.dll

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

options\rpcrt4.dll

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

options\advapi32.dll

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

options\shlwapi.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKLM\

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

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

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

options\ole32.dll

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-0000-000000000046}

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:

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:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9$ 

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9 \setminus 00000004$ 

Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001
Opens key:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004 Opens kev:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007 Opens kev:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000010 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000011 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000000 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000003 HKLM\software\microsoft\windows nt\currentversion\image file execution

Opens kev: options\mswsock.dll

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

options\hnetcfg.dll

 ${\tt HKLM \ } software \verb|\ microsoft \verb|\ rpc \verb|\ paged buffers$ Opens key:

Opens key: HKLM\software\microsoft\rpc

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

options\859ba9477553ccad1bba34c555ab6a1b.exe\rpcthreadpoolthrottle HKLM\software\policies\microsoft\windows nt\rpc Opens key: Opens key: HKLM\software\microsoft\rpc\securityservice

HKLM\system\currentcontrolset\services\winsock\parameters Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll

Opens key: HKLM\system\currentcontrolset\control\computername

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername Opens key: 

cryptographic provider v1.0

Opens key: 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

Opens key:  $HKLM \setminus software \setminus microsoft \setminus cryptography \setminus deshash session keybackward$ 

Opens kev:

9a6f-135d9c6622cc}

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-

a949-c1b91af43b1a}

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

options\n

Opens key: HKCU\software\classes\http

HKCR\http Opens key:

Opens key: HKCU\software\classes\http\curver

Opens key: HKCR\http\curver Opens key: HKCR\http\

Opens key: HKCU\software\classes\http\shell\open

Opens key: HKCR\http\shell\open

HKCU\software\classes\http\shell\open\command Opens key:

Opens key: HKCR\http\shell\open\command Opens key: HKCU\software\classes\http\shell

HKLM\software\classes Opens key: Opens key: HKCU\software\classes\ HKLM\software\microsoft\com3 Opens kev:

Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}

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\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\inprocserver32

 $HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\\\\$ Opens key:

HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-Opens key:

00805fc1270e}\inprocserverx86

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserverx86 Opens key:

Opens kev: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-

00805fc1270e}\localserver32

 $HKCR \ clsid \ \{ba126ae5-2166-11d1-b1d0-00805fc1270e\} \ \ localserver 32$ Opens key:

HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-Opens key:

00805fc1270e}\inprochandler32

HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32 Opens key:

HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-Opens kev:

00805fc1270e}\inprochandlerx86

Opens key:  $HKCR \ clsid \ \{ba126ae5-2166-11d1-b1d0-00805fc1270e\} \ in prochandler x 86 \ and \ barried \ and \$ 

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} Opens kev:

Opens key: HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223} Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\treatas

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas Opens kev: Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprocserver32

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprocserverx86

Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\localserver32

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandler32

 $HKCR \ clsid \ \{33c4643c-7811-46fa-a89a-768597bd7223\} \ \ inprochandler 32$ Opens key:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\inprochandlerx86

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandlerx86 Opens key:

Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-

768597bd7223}\localserver

HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver Opens key: Opens key: HKCU\software\policies\microsoft\windows\network connections HKLM\software\policies\microsoft\windows\network connections Opens kev: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-Opens key:

08002b30309d}\shellfolder

HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder Opens key:

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-

3aea-1069-a2de-08002b30309d}

Opens kev: HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key:

a2de-08002b30309d}

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ clsid \ \{2227a280-microsoft\} \ description \ description$ Opens key:

3aea-1069-a2de-08002b30309d}\shellfolder

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-

3aea-1069-a2de-08002b30309d}\shellfolder

Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d} HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d} Opens key: Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\ Opens key: HKCU\software\microsoft\windows\shellnoroam\muicache\ Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-

00805fc1270e}\shellfolder

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-

3202-11d1-aad2-00805fc1270e}

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ shell compatibility \ objects \ \{7007acc7-3202-11d1-4207acc7-3207acc7-3202-11d1-4207acc7-3$ 

aad2-00805fc1270e}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-

3202-11d1-aad2-00805fc1270e}\shellfolder

 $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus \{7007acc7-the content version \setminus explorer \setminus the content version \setminus explorer \setminus explore$ Opens kev: 3202-11d1-aad2-00805fc1270e}\shellfolder

HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} Opens key:

Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e} HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\ Opens kev:

Opens key:  $HKCR \clsid \footnote{1}{HKCR \clsid \footnote{1}{HKCR \clsid \footnote{1}{KCR \clsid \clsid \footnote{1}{KCR \clsid \clsid$ 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\svstem\wpa\tabletpc Opens key: HKLM\system\wpa\mediacenter

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  $\label{local-operator} \mbox{HKCU\software\mbox{\sc microsoft\windows} nt\current version\app compatflags\layers} \\$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe  $\label{lem:hklm} \verb+Kklm/software/microsoft/windows nt/currentversion/image file execution$ Opens kev: options\version.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens kev: be2efd2c1a33} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89edd5fbde13283 Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57bb813f72dbb91} Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f1 Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus soften \setminus code identifiers \setminus 0 \setminus hashes \setminus \{94e3e076-8f53-42a5-8411-426-8411-426-8411-426-8411-$ 085bcc18a68d} Opens key:  $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-46eb-4fe4-ae2e-46eb-4fe$ b91490411bfc Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 4096 \setminus paths$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 65536 \setminus has hes$ Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 131072 \setminus hashes$ Opens key: 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:

 $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones$ 

Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones Opens kev:

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

 $HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 65536 \ has hes$ Opens kev:

 $HKCU \ software \ \ icrosoft \ \ windows \ safer \ \ code identifiers \ \ \ 65536 \ \ \ urlzones$ Opens kev:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes

Opens kev: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones Opens kev:

 $HKCU \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ \ 262144 \ paths$ Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes Opens key:

 $HKCU \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers \setminus 262144 \setminus urlzones$ 

```
Opens key:
                                                                                                                                       HKCU\software\microsoft\windows\currentversion\explorer\shell folders
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
         Opens key:
options\acgenral.dll
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
        Opens key:
options\winmm.dll
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
                                                                                                                                       \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows nt + current version + image file execution
        Opens key:
 options\shell32.dll
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\drivers32
         Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
                                                                                                                                      HKLM\software\microsoft\oleaut
         Opens kev:
         Opens key:
                                                                                                                                       HKLM\software\microsoft\oleaut\userera
         Opens key:
                                                                                                                                       HKLM\software\microsoft\audiocompressionmanager\drivercache
         Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.ima adpcm
         Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc manager \setminus driver cache \setminus msadpc msa
         Opens key:
                                                                                                                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
         Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
         Opens key:
                                                                                                                                       HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ trspch
         Opens key:
                                                                                                                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
         Opens key:
HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. \ msaudio 1
        Opens key:
 HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
         Opens key:
                                                                                                                                       HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm.iac2
         Opens key:
                                                                                                                                       HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
         Opens key:
                                                                                                                                      HKLM\system\currentcontrolset\control\mediaresources\acm
         Opens key:
                                                                                                                                       HKLM\system\setup
         Opens key:
HKLM\software\microsoft\windows nt\currentversion\image file execution
         Opens key:
options\comctl32.dll
                                                                                                                                       \label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+explorer \verb+\advanced+ \\
         Opens key:
         Opens key:
                                                                                                                                       HKLM\software\microsoft\windows nt\currentversion\languagepack
         Opens kev:
                                                                                                                                       HKLM\system\currentcontrolset\control\productoptions
         Opens key:
                                                                                                                                       HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders
         Opens key:
                                                                                                                                      HKLM\software\policies\microsoft\windows\system
         Opens key:
                                                                                                                                      HKCU\software\microsoft\windows\currentversion\thememanager
         Opens key:
                                                                                                                                       HKLM\system\currentcontrolset\services\sharedaccess
         Opens kev:
                                                                                                                                       HKCU\software\classes\applications\calc.exe
         Opens key:
                                                                                                                                      HKCR\applications\calc.exe
         Opens key:
                                                                                                                                       \label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \textbf{HKLM} \label{thm:local_hammon} \end{tabular} is a software \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \textbf{HKLM} \label{thm:local_hammon} \end{tabular} is a software \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \textbf{HKLM} \label{thm:local_hammon} \end{tabular} is a software \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \textbf{HKLM} \label{thm:local_hammon} \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \label{thm:local_hammon} \end{tabular} \begin{tabular}{ll} HKLM \label{thm:local_hammon} \label{thm:l
         Opens key:
                                                                                                                                       HKLM\software\microsoft\ctf\tip\
                                                                                                                                      HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 80
         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}
                                                                                                                                       HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
         Opens key:
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}
                                                                                                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
        Opens key:
 c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
         Opens key:
                                                                                                                                      HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
         Opens key:
                                                                                                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
 c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
        Opens key:
                                                                                                                                      HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
         Opens key:
                                                                                                                                      HKLM \setminus software \setminus microsoft \setminus tip \setminus \{1188450c - fdab - 47ae - 80d8 - 8
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
         Opens key:
                                                                                                                                       HKLM \setminus software \setminus icrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc
 77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
        Opens key:
                                                                                                                                      HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
 c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
         Opens key:
                                                                                                                                      HKLM \setminus software \setminus microsoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fcc-854c-4fc
77e8f3d1aa80\} \land (c6debc0a-f2b2-4f17-930e-ca9faff4cd04) \land (c6debc0a-f2b2-4f17-95aff4cd04) \land (
         Opens key:
                                                                                                                                       \label{lem:hkcu-appevents-schemes-apps-lemontification-current} \\ \text{Hkcu-appevents-schemes-apps-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \\ \\ \text{Hkcu-app-lemontification-current} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\
```

Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre\_initialize[disablemetafiles] Oueries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[859ba9477553ccad1bba34c555ab6a1b] Oueries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[859ba9477553ccad1bba34c555ab6a1b] HKLM\software\microsoft\windows nt\currentversion\windows[appinit dlls] Oueries value: Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack] Oueries value: HKCU\control panel\desktop[multiuilanguageid] Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout] HKLM\software\microsoft\ole[rwlockresourcetimeout] Oueries value: Queries value: HKCR\interface[interfacehelperdisableall] Queries value: HKCR\interface[interfacehelperdisableallforole32] HKCR\interface[interfacehelperdisabletypelib] Oueries value: Queries value: HKCR\interface\{00020400-0000-0000-c000-00000000046}[interfacehelperdisableall] HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableallforole32] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version] HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9[serial access num] Oueries value: Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000002[packedcatalogitem] Oueries value: Queries value: Queries value:  $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 000000000005 \ [packed catalog item]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000011[packedcatalogitem] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace catalog5[num catalog entries] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath] Queries value: Queries value: Queries value: Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog S \setminus catalog\_entries \setminus 000000000001[providerid]$ 

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ (catalog\_entries \ 00000000001 \ [address family]$ 

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace \_ catalog 5 \ catalog\_entries \ 000000000001 [supported names pace]$ 

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storesserviceclassinfo] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000002[librarypath] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid] Queries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000002 [address family])$ Queries value:

```
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
    Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ winsock 2 \ parameters \ namespace\_catalog \ services \ namespace\_catalog \ namespac
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
    Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
    Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 000000000003 [supported namespace]
    Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_\catalog_entries\00000000003[storesserviceclassinfo]
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
    Queries value:
                                                       HKLM\software\microsoft\rpc[maxrpcsize]
    Oueries value:
                                                       HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
                                                        HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Queries value:
                                                       HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Oueries value:
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
    Queries value:
HKLM \verb| system| current control \verb| set| computer name| active computer name| [computer name] | for the computer name active computer name active computer name] | for the computer name active na
    Queries value:
                                                       HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
    Queries value:
                                                       HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
                                                       HKLM\system\currentcontrolset\control\session
    Queries value:
manager[safeprocesssearchmode]
    Queries value:
                                                        HKLM\software\microsoft\cryptography[machineguid]
                                                       HKCR\http\shell\open\command[]
    Oueries value:
    Queries value:
                                                       HKLM\software\clients\startmenuinternet[]
                                                        HKLM\software\microsoft\com3[regdbversion]
    Oueries value:
                                                        HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid]
    Oueries value:
    Queries value:
                                                       HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[dllsurrogate]
                                                        HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[localservice]
    Queries value:
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-
    Oueries value:
768597bd7223}\inprocserver32[inprocserver32]
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
    Queries value:
                                                       HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[appid]
    Oueries value:
    Oueries value:
                                                       HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[wantsfordisplay]
                                                       HKCR\clsid\{2227a280-3aea-1069-a2de-
    Queries value:
08002b30309d}\shellfolder[attributes]
                                                       HKCR\clsid\{2227a280-3aea-1069-a2de-
    Queries value:
08002b30309d}\shellfolder[callforattributes]
    Oueries value:
08002b30309d}1
                                                       HKCR\clsid\{2227a280-3aea-1069-a2de-
    Queries value:
08002b30309d}\shellfolder[hidefolderverbs]
                                                       HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
    Oueries value:
    Queries value:
HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\ windows \ system 32 \ shell 32.dll, -9319] \ moreover \ mor
                                                       HKCR\clsid\{7007acc7-3202-11d1-aad2-
   Oueries value:
00805fc1270e}\shellfolder[wantsfordisplay]
    Queries value:
                                                       HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[attributes]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{7007acc7-3202-11d1-aad2-
00805fc1270e}1
    Oueries value:
                                                       HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[hidefolderverbs]
                                                       HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
    Oueries value:
    Queries value:
```

 $HKCU \ software \ microsoft \ windows \ shell no roam \ muicache [@c:\ windows \ system 32 \ net shell. dll, -1200] \ dll, -1200] \ dll, -1200] \ dll, -1200]$ 

Queries value: HKLM\system\currentcontrolset\control\session

manager\appcompatibility[disableappcompat]

Queries value: HKLM\system\wpa\mediacenter[installed]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[current\_protocol\_catalog]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [current\_namespace\_catalog]$ 

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]

Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ paths \ \{dda3f824-d8cb-441b-834d-be2efd2c1a33\} \ [saferflags]$ 

Queries value:

Queries value:

 $HKLM software \verb|\policies| incrosoft| windows \verb|\safer| code identifiers| 0 hashes | \{349d35ab-37b5-462f-9b89-edd5fbde 1328\} | hashalg | 128b hashelg | 12$ 

Queries value:

 $HKLM software \\policies \\microsoft \\windows \\safer \\code identifiers \\0 \\hashes \\\{349d35ab-37b5-462f-9b89-edd5fbde \\1328\} \\ [itemsize]$ 

Queries value:

 $HKLM software \verb|\policies| incressft \verb|\windows| safer| code identifiers \verb|\olicies| add 5 ab-37 b5-462 f-9 b89-edd 5 fbde 1328 [safer flags]$ 

Oueries value

Oueries value:

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\{itemsize}

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{7fb9cd2e-3076-4df9-a57b-b813f72dbb91\} \ [saferflags]$ 

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16d-7c29ddecae3f\} [item data]$ 

Queries value:

Queries value:

 $HKLM \ software \ blicies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{81d1fe15-dd9d-4762-b16d-7c29ddecae3f\} [itemsize]$ 

Queries value:

Queries value:

 $\label{thm:local} $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}\ [itemdata]$ 

Queries value:

 $HKLM \ software \ blicies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} \ [hashalg]$ 

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{94e3e076-8f53-42a5-8411-085bcc18a68d\} [itemsize]$ 

Queries value:

Queries value:

 $HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}\[itemdata]$ 

Queries value:

 $HKLM \ software \ b01icies \ icrosoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} \ [hashalg]$ 

Queries value:

 $HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ 0 \ hashes \ \{dc971ee5-44eb-4fe4-ae2e-b91490411bfc\} [itemsize]$ 

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell

folders[cache]

Oueries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename] Oueries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd] Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave31 Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9] Oueries value: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3] Queries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9] Oueries value:  $\label{lem:hkcu} \verb+KKCU \software \verb+ microsoft \verb+ multimedia \verb+ audio [system formats]+ \\$ Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.imaadpcm] Queries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache] Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags] HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.msadpcm] HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport] Oueries value: Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msg711] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]  $\label{thm:local_hamma} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} and $$ ion manager \end{tabular} and $$ ion manager \end{tabular} $$ ion m$ Queries value:  $HKLM \label{lem:hklm} White the large statement of the large state$ Oueries value:  $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox| msg711[cfiltertags]$ Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.msgsm610]

Queries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]

Oueries value:

Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache] Oueries value:  $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ msgsm610[cfilter tags]$ HKLM\software\microsoft\windows Oueries value: nt\currentversion\drivers32[msacm.trspch] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport] Oueries value: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags] Oueries value:

Oueries value:

HKLM\software\microsoft\windows Queries value:

nt\currentversion\drivers32[msacm.msg723]

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport] Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache] Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]

HKLM\software\microsoft\windows Queries value:

nt\currentversion\drivers32[msacm.msaudio1]

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport] Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags] Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.sl\_anet]

Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[fdwsupport]

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[cformattags] Oueries value:

Oueries value:

HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2] Oueries value:

Queries value:

 $HKLM \verb|\software\microsoft\audiocompressionmanager\drivercache\mbox| msacm.iac2[fdwsupport]|$ 

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags] Queries value:

 $HKLM \ software \ microsoft \ audio compression manager \ driver cache \ mac a cache]$ Oueries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]

HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm] Oueries value:

Oueries value:

 $HKLM \setminus software \setminus microsoft \setminus audio compression manager \setminus driver cache \setminus msacm. 13 acm[cformattags]$ Oueries value:

Queries value:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.13acm[cfiltertags] HKCU\software\microsoft\multimedia\audio compression

Queries value: manager\msacm[nopcmconverter]

HKCU\software\microsoft\multimedia\audio compression manager\priority

Queries value:

v4.00[priority1] Queries value: HKLM\system\setup[systemsetupinprogress] Oueries value: HKCU\control panel\desktop[smoothscroll]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]

Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[userenvdebuglevel]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\winlogon[chkaccdebuglevel]

Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[personal]

Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local settings]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\winlogon[rsopdebuglevel]

HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging] Oueries value: Queries value:  $\label{lem:hkcu} \verb+KKCU \software \verb+microsoft \verb+windows \verb+current version \verb+ the memanager [compositing]+ \\$  Queries value: HKCU\control panel\desktop[lamebuttontext]

HKLM\system\currentcontrolset\services\sharedaccess[start] Oueries value:

Oueries value:

HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe] Oueries value:

 $HKLM \verb|\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]|$ Oueries value:  $HKLM \setminus software \setminus irrosoft \setminus tip \setminus \{78cb5b0e-26ed-4fcc-854c-4fcc$ 

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-Oueries value:

77e8f3d1aa80\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]

Queries value: HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-

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] HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-Oueries value:

77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]

Queries value: HKCU\appevents\schemes\apps\.default\systemnotification\.current[]

Sets/Creates value:  $HKCU \setminus software \setminus classes \setminus clsid \setminus \{fbeb8a05-beee-4442-804e-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-4446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-446-beee-466-beee-$ 

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.exe]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]

Value changes:  $HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]$ 

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog\_entries\0000000000010[packedcatalogitem]

Value changes:

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000007[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\000000000004[packedcatalogitem]

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem]

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\00000000001[packedcatalogitem]

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]

Value changes:

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

Value changes: HKCU\sessioninformation[programcount]