Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3328, Task ID: 822

Task ID: 822 Risk Level: 7

Date Processed: 2016-05-18 10:42:16 (UTC)

Processing Time: 62.48 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe"

Sample ID: 3328 Type: basic Owner: admin

Label: 6ff8b3dc9a34dc40e47ff4c3444c8241

Date Added: 2016-05-18 10:30:51 (UTC)

File Type: PE32:win32:gui File Size: 94240 bytes

MD5: 6ff8b3dc9a34dc40e47ff4c3444c8241

SHA256: 22dd9934836541b81983ef5ed7abb4d82edd6afcdc272f027f8bffb41145fac9

Description: None

Pattern Matching Results

6 Modifies registry autorun entries

2 PE: Nonstandard section

5 Installs service

Disables system restoreAdds autostart object

5 PE: Contains compressed section

3 Long sleep detected

Static Events

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

Process/Thread Events

Creates process: C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe

["C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\0CEC5634AEA14E6600000CEC494D5354

 $\label{lem:continuous} Creates\ mutex: \qquad \verb|\Sessions|1| BaseNamedObjects| CicLoadWinStaWinStaO| \\$

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event: \Security\LSA_AUTHENTICATION_INITIALIZED
Creates event: \KernelObjects\MaximumCommitCondition

Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates:

C:\ProgramData\0CEC5634AEA14E6600000CEC494D5354\0CEC5634AEA14E6600000CEC494D5354

Creates: C:\ProgramData\0CEC5634AEA14E6600000CEC494D5354

Creates:

C:\ProgramData\OCEC5634AEA14E6600000CEC494D5354\OCEC5634AEA14E6600000CEC494D5354.exe

Creates:

C:\ProgramData\OCEC5634AEA14E6600000CEC494D5354\OCEC5634AEA14E6600000CEC494D5354.ico

Opens: C:\Windows\Prefetch\6FF8B3DC9A34DC40E47FF4C3444C8-B42B5CB2.pf

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dl1

 Opens:
 C:\Windows\System32\wow64win.dl1

 Opens:
 C:\Windows\System32\wow64cpu.dl1

 Opens:
 C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost

Opens: C:\Windows\SysWOW64\sechost.dll

Opens: C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe.Local\

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

 $Opens: C: \verb|Windows| winsxs| x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\\ \verb|comctl32.dl1|$

Opens: C:\Windows\SysWOW64\imm32.dll

Opens: C:\Windows\SysWOW64\activeds.dll

Opens: C:\Windows\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe

 Opens:
 C:\windows\temp\VERSION.dll

 Opens:
 C:\Windows\SysWOW64\version.dll

 Opens:
 C:\windows\temp\MSIMG32.dll

 Opens:
 C:\Windows\SysWOW64\msimg32.dll

 Opens:
 C:\windows\temp\Secur32.dll

 Opens:
 C:\Windows\SysWOW64\secur32.dll

```
C:\windows\temp\WINHTTP.dll
Opens:
Opens:
                        C:\Windows\SysWOW64\winhttp.dll
                        C:\windows\temp\webio.dll
Opens:
Opens:
                        C:\Windows\SysWOW64\webio.dll
Opens:
                        C:\Windows\SysWOW64\rpcss.dll
Opens:
                        C:\Windows\SysWOW64\uxtheme.dll
Opens:
                        C:\windows\temp\profapi.dll
Opens:
```

Opens: C:\Windows\SysWOW64\profapi.dll

Opens:

C:\ProgramData\0CEC5634AEA14E6600000CEC494D5354\0CEC5634AEA14E6600000CEC494D5354

Opens: C:\ProgramData

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls C:\Windows\SysWOW64\en-US\KernelBase.dll.mui Opens: Opens: C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe

Opens: C:\windows\temp\cryptsp.dll C:\Windows\SysWOW64\cryptsp.dll Opens: Opens: C:\windows\temp\credssp.dll Opens: C:\Windows\SysWOW64\credssp.dll C:\Windows\SysWOW64\rsaenh.dll Opens: Opens: C:\windows\temp\RpcRtRemote.dll C:\Windows\SysWOW64\RpcRtRemote.dll Opens: C:\Windows\SysWOW64\mswsock.dll Opens: Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL

Opens: C:\windows\temp\SXS.DLL C:\Windows\SysWOW64\sxs.dll Opens: Opens: C:\windows\temp\DNSAPI.dll Opens: C:\Windows\SysWOW64\dnsapi.dll Opens:

C:\ProgramData\0CEC5634AEA14E6600000CEC494D5354\0CEC5634AEA14E6600000CEC494D5354.exe

Opens: C:\Windows\SysWOW64\ieframe.dll C:\Windows\SysWOW64\stdole2.tlb Opens: Opens: C:\Windows\SysWOW64\tzres.dll

Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui

Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\Fonts\arial.ttf Opens: C:\windows\temp\dwmapi.dll C:\Windows\SysWOW64\dwmapi.dll Opens:

Opens: C:\Windows\SysWOW64\uxtheme.dll.Config

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

C:\Windows\winsxs\x86_microsoft.windows.common-Opens: controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

C:\Windows\WindowsShell.Manifest Opens: Opens: C:\Windows\Fonts\arialbd.ttf Opens: C:\Windows\SysWOW64\oleacc.dll Opens: C:\windows\temp\OLEACCRC.DLL C:\Windows\SysWOW64\oleaccrc.dll Opens:

Writes to:

C:\ProgramData\OCEC5634AEA14E6600000CEC494D5354\OCEC5634AEA14E6600000CEC494D5354.exe

C:\ProgramData\0CEC5634AEA14E6600000CEC494D5354\0CEC5634AEA14E6600000CEC494D5354

Writes to:

C:\ProgramData\OCEC5634AEA14E6600000CEC494D5354\OCEC5634AEA14E6600000CEC494D5354.ico

Reads from: C:\Windows\SysWOW64\activeds.dll

Reads from: C:\Windows\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe

Reads from: C:\Windows\SysWOW64\ieframe.dll Reads from: C:\Windows\SysWOW64\stdole2.tlb

Network Events

175.41.29.181:80 Connects to: Sends data to: 175.41.29.181:80

Windows Registry Events

Creates key: HKLM\software\wow6432node\microsoft\security center Creates key: HKLM\software\wow6432node\microsoft\security center\svc

Creates key: HKLM\software\wow6432node

Creates key: HKLM\software\wow6432node\microsoft

Creates key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Creates key: HKLM\system\currentcontrolset\services\luafv HKLM\software\wow6432node\microsoft\windows Creates key:

nt\currentversion\systemrestore

Creates key:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\system

Creates key: HKLM\software\microsoft\windows\currentversion\policies\system

Creates key: HKLM\software\wow6432node\microsoft\windows defender HKLM\system\currentcontrolset\services\tcpip\parameters Creates key: Creates key: HKCU\software\microsoft\windows\currentversion\runonce

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

options

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\wow64 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

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

Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

Opens key: HKLM\system\currentcontrolset\control\nls\customlocale Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

HKCU\ Opens kev:

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side \setminus assembly storage roots$

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: Opens key: HKLM\system\currentcontrolset\services\crypt32 Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\gre_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows Opens key:

Opens key: HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing HKLM\software\microsoft\ole\tracing Opens key:

Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKLM\software\wow6432node\microsoft\rpc

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

Opens key:

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens kev: HKLM\software\microsoft\sqmclient\windows

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

Opens kev:

Opens key:

 $HKLM \label{lem:hklm} Which was the statement of the st$

fdc1-4dc3-a9dd-070d1d495d97}

Opens key:

fdc1-4dc3-a9dd-070d1d495d97}\propertybag

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\profilelist

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\wow6432node\microsoft\internet explorer

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus internet$ Opens key:

settings\winhttp\tracing

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\winhttp

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\30f56ab0 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001

Opens key:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
   Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ parameters \ protocol\_catalog\_entries \ protocol\_catalog \ parameters \ parameters
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
   Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
   Opens key:
                                             HKLM\system\currentcontrolset\control\cmf\config
   Opens key:
                                             HKCU\software\classes\
   Opens key:
                                             HKLM\software\microsoft\com3
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}
                                             HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
   Opens key:
00a0c90a8f39}\treatas
                                             HKCR\wow6432 node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treat as
   Opens key:
                                             HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
   Opens kev:
00a0c90a8f39}\progid
                                             HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
   Opens kev:
                                             HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
   Opens key:
   Opens key:
                                             HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
   Opens key:
                                             HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\progid
   Opens key:
                                             HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\progid
                                             HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
   Opens kev:
00a0c90a8f39}\inprocserver32
   Opens key:
                                             HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
                                             HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
  Opens key:
00a0c90a8f39}\inprochandler32
   Opens key:
                                             HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
                                             HKCU\software\classes\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
   Opens key:
00a0c90a8f39}\inprochandler
  Opens key:
                                             HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler
   Opens key:
                                             HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
   Opens kev:
                                             HKLM\svstem\currentcontrolset\control\securityproviders
   Opens key:
                                             HKCU\software\classes\appid\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
   Opens key:
                                             HKCR\appid\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
   Opens key:
                                             HKLM\software\wow6432node\microsoft\ole\appcompat
   Opens key:
                                             HKLM\software\microsoft\ole\appcompat
   Opens key:
                                             HKLM\system\currentcontrolset\control\lsa
   Opens kev:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
   Opens key:
                                             HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
   Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
   Opens kev:
                                             HKLM\software\policies\microsoft\cryptography
   Opens key:
                                             HKLM\software\microsoft\cryptography
   Opens key:
                                             HKLM\software\wow6432node\microsoft\cryptography\offload
   Opens key:
                                             HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
   Opens key:
                                             \label{local-bound} \mbox{HKCR} $$ \mbox{Wow} 6432 \mbox{node} \mbox{interface} \mbox{\{00000134-0000-0000-c000-000000000046\}} $$
                                             HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{00000134-0000-0000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c000-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-
   Opens kev:
```

00000000046}\proxystubclsid32

```
HKCR\wow6432node\interface\{00000134-0000-0000-c000-
      Opens key:
00000000046}\proxystubclsid32
                                                                                              HKLM\software\wow6432node\microsoft\rpc\extensions
      Opens kev:
      Opens key:
                                                                                              HKLM\software\microsoft\rpc\extensions
      Opens key:
                                                                                              HKLM\system\currentcontrolset\control\lsa\sspicache
                                                                                              Opens key:
      Opens key:
                                                                                              HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
                                                                                              HKLM\system\currentcontrolset\services\bfe
      Opens key:
                                                                                              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
      Opens key:
settings\connections
      Opens kev:
                                                                                              HKLM\software\microsoft\samclient\windows\disabledprocesses\
      Opens key:
                                                                                              HKLM\software\microsoft\sqmclient\windows\disabledsessions\
      Opens key:
                                                                                              HKLM\system\currentcontrolset\services\winsock\parameters
      Opens key:
                                                                                              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
      Opens key:
                                                                                              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
      Opens key:
                                                                                              HKLM\system\currentcontrolset\services\winsock\setup migration\providers
      Opens key:
                                                                                              HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}
      Opens key:
                                                                                              HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
      Opens key:
                                                                                              HKCU\software\classes\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
                                                                                              HKCR\wow6432 node\interface \ \{85cb6900-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d95-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-96
      Opens key:
0080c7f4ee85}\proxystubclsid32
      Opens key:
                                                                                              HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}
                                                                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}
      Opens key:
      Opens key:
                                                                                              HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{00020424-0000-0000-c000-c000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c0000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c000-c00-c000-c000-c000-c000-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00-c00
000000000046}\treatas
      Opens key:
                                                                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}\treatas
      Opens key:
                                                                                              HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\progid
                                                                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-00000000046}\progid
      Opens key:
      Opens key:
                                                                                              HKCU\software\classes\clsid\{00020424-0000-0000-c000-00000000046}
                                                                                              HKCR\clsid\{00020424-0000-0000-c000-00000000046}
      Opens key:
                                                                                              Opens key:
000000000046}\progid
      Opens key:
                                                                                              HKCR\clsid\{00020424-0000-0000-c000-00000000046}\progid
      Opens key:
                                                                                              HKCU\software\classes\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32
      Opens key:
                                                                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
00000000046}\inprocserver32
      Opens key:
                                                                                              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
      Opens key:
                                                                                              00000000046}\inprochandler32
      Opens key:
                                                                                              HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
      Opens key:
                                                                                              00000000046}\inprochandler
                                                                                              HKCR \setminus wow 6432 \\ node \\ \clsid \\ \cl
      Opens key:
000000000046}\inprochandler
      Opens key:
                                                                                              HKLM\system\currentcontrolset\services\dnscache\parameters
      Opens key:
                                                                                              HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
      Opens key:
                                                                                              HKLM\software\policies\microsoft\windows nt\dnsclient
      Opens kev:
                                                                                              HKLM\svstem\currentcontrolset\services\dns
                                                                                              HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{85cb6900-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d95-11cf-960c-4d9-11cf-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-4d9-960c-
      Opens key:
0080c7f4ee85}\forward
      Opens key:
                                                                                              HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
      Opens key:
                                                                                              HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
                                                                                              HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
      Opens key:
      Opens key:
                                                                                              HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus interface \setminus \{85cb6900 - 4d95 - 11cf - 960c - 
0080c7f4ee85}\typelib
                                                                                              HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
      Opens key:
0080c7f4ee85}\typelib
      Opens key:
                                                                                              HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
                                                                                              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
      Opens key:
      Opens key:
                                                                                              HKCU \setminus software \setminus classes \setminus typelib \setminus \{eab22ac0-30c1-11cf-a7eb-0000c05bae0b\} \setminus 1.1 + (ab22ac0-30c1-11cf-a7eb-0000c05bae0b) \setminus 1.1 + (ab22ac0-30c1-11cf-a7eb-000
      Opens key:
                                                                                              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
      Opens key:
                                                                                              HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
      Opens key:
                                                                                              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
                                                                                              HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
      Opens key:
0000c05bae0b}\1.1\0\win32
      Opens key:
                                                                                              HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
                                                                                              HKCU\software\classes\typelib
      Opens key:
      Opens key:
      Opens key:
                                                                                              HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
                                                                                              HKCR\typelib\{00020430-0000-0000-c000-00000000046}
      Opens key:
      Opens key:
                                                                                              HKCU\software\classes\typelib\{00020430-0000-0000-c000-00000000046}\2.0
```

HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0

HKCU\software\classes\typelib\{00020430-0000-0000-c000-

Opens key: Opens key:

```
000000000046}\2.0\0
```

Opens key: HKCR\typelib\{00020430-0000-0000-000000000046}\2.0\0
Opens key: HKCU\software\classes\typelib\{00020430-0000-0000-c000-

00000000046}\2.0\0\win32

Opens key: HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32

Opens key: HKLM\software\wow6432node\policies\microsoft\windows

nt\dnsclient\dnspolicyconfig

Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig

Opens key:

HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig

Opens key: HKCU\software\classes\wow6432node\interface\{00020400-0000-0000-c000-

00000000046}

00000000046}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{00020400-0000-0000-c000-

00000000046}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-

000000000046}

000000000046}\treatas

 Opens key:
 HKCR\wow6432node\clsid\{00020420-0000-0000-0000-000000000046}\treatas

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000

000000000046}\progid

000000000046}\progid

Opens key: HKCR\clsid\{00020420-0000-0000-c000-00000000046}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-

00000000046}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-

00000000046}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-

000000000046}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-

00000000046}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{00020420-0000-0000-c000-

00000000046}\inprochandler

Opens key: HKCR\wow6432node\clsid\{00020420-0000-0000-c000-

000000000046}\inprochandler

Opens key: HKCU\software\classes\wow6432node\interface\{b196b284-bab4-101a-b69c-

00aa00341d07}

 Opens key:
 HKCR\wow6432node\interface\{b196b284-bab4-101a-b69c-00aa00341d07}

 Opens key:
 HKCU\software\classes\wow6432node\interface\{b196b284-bab4-101a-b69c-00aa00341d07}

00aa00341d07}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{b196b284-bab4-101a-b69c-

00aa00341d07}\proxystubclsid32

Opens key: HKCU\software\classes\wow6432node\interface\{b196b286-bab4-101a-b69c-

 00aa00341d07}
 HKCR\wow6432node\interface\{b196b286-bab4-101a-b69c-00aa00341d07}

 Opens key:
 HKCU\software\classes\wow6432node\interface\{b196b286-bab4-101a-b69c-00aa00341d07}

00aa00341d07}\proxystubclsid32

Opens key: HKCR\wow6432node\interface\{b196b286-bab4-101a-b69c-

00aa00341d07}\proxystubclsid32

Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

Opens key:

HKLM\software\wow6432node\microsoft\ctf\compatibility\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-

Opens key: HKLM\software\wow6432node\microsoft\ctf\

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\fontsubstitutes

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\treatas

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprocserver32

HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-Opens key:

00c04fd705a2}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler32

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler32

 $HKCU \setminus software \setminus classes \setminus wow6432 node \setminus clsid \setminus \{8856f961-340a-11d0-a96b-1440a-11d0-a96b-1440a-14$ Opens key:

00c04fd705a2}\inprochandler

Opens key: HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-

00c04fd705a2}\inprochandler

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\svstem\currentcontrolset\control\terminal server[tsuserenabled]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] HKLM\system\currentcontrolset\control\nls\customlocale[empty] Queries value:

Queries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value:

HKLM\system\currentcontrolset\control\mui\uilanguages\en-Queries value:

us[alternatecodepage]

HKCU\control panel\desktop[preferreduilanguages] Queries value:

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]]$ HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

HKLM\software\microsoft\windows Queries value: nt\currentversion\gre_initialize[disablemetafiles]

Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[6ff8b3dc9a34dc40e47ff4c3444c8241] Oueries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit dlls]

HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress] HKLM\system\setup[systemsetupinprogress] Oueries value:

HKLM\software\microsoft\sqmclient\windows[ceipenable] Queries value:

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

fdc1-4dc3-a9dd-070d1d495d97}[category]

Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[name]

fdc1-4dc3-a9dd-070d1d495d97}[parentfolder] Oueries value:

fdc1-4dc3-a9dd-070d1d495d97}[description]

fdc1-4dc3-a9dd-070d1d495d97}[relativepath]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[parsingname]

fdc1-4dc3-a9dd-070d1d495d97}[infotip]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[localizedname]

fdc1-4dc3-a9dd-070d1d495d97}[icon]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[security]

fdc1-4dc3-a9dd-070d1d495d97}[streamresource]

Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]

Oueries value: HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\\62ab5d82fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly] fdc1-4dc3-a9dd-070d1d495d97}[roamable] Oueries value: fdc1-4dc3-a9dd-070d1d495d97}[precreate] Oueries value: fdc1-4dc3-a9dd-070d1d495d97}[stream] Oueries value: fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath] Oueries value: fdc1-4dc3-a9dd-070d1d495d97}[attributes] Oueries value: $\label{thm:local_explorer_local_ex$ fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid] Queries value:

fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]

Queries value: HKLM\software\microsoft\windows

 $\verb|nt\currentversion\profile| list[programdata]|$

Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\internet explorer[version]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\winhttp\tracing[enabled]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[sharecredswithwinhttp]

Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\winhttp[disablebranchcache]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]

Queries value:

 $HKLM \land system \land current control set \land services \land winsock 2 \land parameters \land protocol_catalog 9 [serial_access_num]$

Queries value:

Queries value:

Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 000000000001 \ [packed catalog item] \\ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000002[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 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]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Oueries value:

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
Oueries value:

 $HKLM \ system \ (current controls et\ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ name space_catalog \ name space_catalog$

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Queries 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:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ solves \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \000000000004 \[version] \queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000005 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \shape \current \shape \s$

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
  Oueries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 0000000000006 [supported name space]]
  Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus names pace\_catalog \\ \setminus catalog\_entries \setminus 000000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000006[storesserviceclassinfo]
  Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog \\ \setminus catalog\_entries \setminus 0000000000006[provider info]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
                                    HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
                                    HKLM\software\microsoft\com3[com+enabled]
  Queries value:
                                    HKCR\wow6432node\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[]
  Oueries value:
                                   HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
                                    HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
  Queries value:
                                    HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
                                    \label{localized} \verb|HKLM\system\currentcontrolset\control\lsa[everyoneincludes an onymous]| | The property of the property o
  Queries value:
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
                                    HKLM\system\currentcontrolset\control\session
  Queries value:
manager[safeprocesssearchmode]
                                    HKLM \setminus system \setminus current control \setminus lsa \setminus fipsal gorithm policy [enabled]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
                                    HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Oueries value:
  Oueries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
                                    HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:
  Oueries value:
                                    HKLM\software\microsoft\cryptography[machineguid]
                                    HKCR\wow6432node\interface\{00000134-0000-0000-c000-
  Queries value:
00000000046}\proxystubclsid32[]
                                   HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Queries value:
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Oueries value:
  Queries value:
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
                                    HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Oueries value:
  Oueries value:
HKLM\system\currentcontrol\set\control\lsa\sspicache\credssp.dll[tokensize]
                                    HKLM\software\microsoft\rpc\extensions[remoterpcdll]
  Queries value:
                                    HKLM\software\wow6432node\microsoft\windows\currentversion\internet
  Oueries value:
settings\connections[winhttpsettings]
  Queries value:
                                   HKLM\software\microsoft\sqmclient\windows\disabledprocesses[10b1e396]
  Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
                                   Queries value:
                                    HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:
                                    HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32[]
  Queries value:
                                    HKCR \setminus \{00020424-0000-0000-c000-000000000046\}[]
                                    HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
  Oueries value:
00000000046}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
  Oueries value:
000000000046}\inprocserver32[]
  Queries value:
                                   HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
```

```
HKCR\wow6432node\clsid\{00020424-0000-0000-c000-
 Oueries value:
00000000046}\inprocserver32[threadingmodel]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
                        HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
 Queries value:
0080c7f4ee85}\typelib[]
                       HKCR\wow6432node\interface\{85cb6900-4d95-11cf-960c-
 Oueries value:
0080c7f4ee85}\typelib[version]
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
 Queries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
HKLM\svstem\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
 Queries value:
                       HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
                       HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
 Queries value:
HKLM \verb|\system| current controlset \verb|\services| tcpip \verb|\parameters[disable dynamic update]|
 Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
 Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [disable reverse address registrations]
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
 Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
 Queries value:
Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration refreshinter val]
 Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
 Oueries value:
Oueries value:
```

```
Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
    Oueries value:
                                                             HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
    Oueries value:
                                                             HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
    Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
    Queries value:
    Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [use compartments]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
    Queries value:
HKLM \ system \ (current control set \ services \ dns cache \ parameters \ [resolver registration]
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
                                                            HKCR\typelib\{00020430-0000-0000-c000-00000000046}\2.0\0\win32[]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:
                                                            HKLM\software\microsoft\rpc[udtalignmentpolicy]
    Queries value:
                                                            HKCR\wow6432node\interface\{00020400-0000-0000-c000-
00000000046}\proxystubclsid32[]
                                                            HKCR \setminus wow6432 \\ node \\ \clsid \\ \cls
    Queries value:
                                                            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
    Oueries value:
00000000046}\inprocserver32[inprocserver32]
                                                            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
    Queries value:
000000000046}\inprocserver32[]
    Oueries value:
                                                            HKCR\wow6432node\clsid\{00020420-0000-0000-c000-
00000000046}\inprocserver32[threadingmodel]
    Queries value:
                                                            HKCR\wow6432node\interface\{b196b284-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32[]
    Oueries value:
                                                            HKCR\wow6432node\interface\{b196b286-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32[]
    Queries value:
                                                            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
                                                            HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
    Queries value:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
    Oueries value:
                                                            HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
                                                             HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Oueries value:
    Queries value:
                                                            HKLM\system\currentcontrolset\control\nls\language groups[1]
    Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced [usedoubleclick timer]) \ described a software \ described \ described a software \ described a software \ described \ descr
                                                            HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
    Oueries value:
ui]
                                                             HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial]
    Oueries value:
    Oueries value:
                                                             HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
    Queries value:
                                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
    Queries value:
                                                             HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
    Queries value:
                                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[]
                                                            HKCR\wow6432node\clsid\{8856f961-340a-11d0-a96b-
    Oueries value:
00c04fd705a2}\inprocserver32[threadingmodel]
    Sets/Creates value:
                                                            HKLM\software\wow6432node\microsoft\security center[antivirusoverride]
    Sets/Creates value:
                                                            HKLM\software\wow6432node\microsoft\security center[firewalloverride]
    Sets/Creates value:
```

HKCU\software\microsoft\windows\currentversion\policies\explorer[hidescahealth]

Sets/Creates value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\systemrestore[rpsessioninterval]

Sets/Creates value:

HKCU\software\microsoft\windows\currentversion\runonce[0cec5634aea14e6600000cec494d5354]

Value changes: HKLM\software\wow6432node\microsoft\security

center[antivirusdisablenotify]

Value changes: HKLM\software\wow6432node\microsoft\security

center[firewalldisablenotify]

Value changes: HKLM\software\wow6432node\microsoft\security

center[updatesdisablenotify]

Value changes: HKLM\system\currentcontrolset\services\luafv[start]

Value changes:

HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]

Value changes:

HKLM\software\microsoft\windows\currentversion\policies\system[consentpromptbehavioradmin]

Value changes: HKLM\software\wow6432node\microsoft\windows defender[disableantispyware]

Value changes: HKLM\software\wow6432node\microsoft\security center[antivirusoverride]

Value changes: HKLM\software\wow6432node\microsoft\security center[firewalloverride]

Value changes:

 $HKCU \ software \ microsoft \ windows \ current version \ policies \ explorer [hidescahealth]$

Value changes: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\systemrestore[rpsessioninterval]

Value changes:

HKCU\software\microsoft\windows\currentversion\runonce[Ocec5634aea14e6600000cec494d5354]