Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 203, Task ID: 810

Task ID: 810 Risk Level: 3

Date Processed: 2016-04-28 13:09:53 (UTC)

Processing Time: 61.15 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\9a992314512bbc93b07328b3941fe048.exe"

Sample ID: 203 Type: basic Owner: admin

Label: 9a992314512bbc93b07328b3941fe048

Date Added: 2016-04-28 12:45:11 (UTC)

File Type: PE32:win32:gui File Size: 925112 bytes

MD5: 9a992314512bbc93b07328b3941fe048

SHA256: 72668272001346e2deb5d2f4ff6836f7a6a613a25dfcf456c61ed1adc3ef03ef

Description: None

Pattern Matching Results

3 Writes to a log file [Info]

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\9a992314512bbc93b07328b3941fe048.exe

["C:\windows\temp\9a992314512bbc93b07328b3941fe048.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\DirectSound DllMain mutex (0x00000AA0)

Creates mutex: \BaseNamedObjects\RCPHost_Instance_Mutex

Creates event: \Sessions\1\BaseNamedObjects\EClientDisconnect10902937

Creates event: \Sessions\1\BaseNamedObjects\DINPUTWINMM

File System Events

Creates: C:\ProgramData

Creates: C:\ProgramData\Remote Control PC

Creates: C:\ProgramData\Remote Control PC\apc-host.log
Creates: C:\ProgramData\Remote Control PC\hostaccount.ini
Creates: C:\ProgramData\Remote Control PC\hoststate.dat

Opens: C:\Windows\Prefetch\9A992314512BBC93B07328B3941FE-B154F679.pf

Opens: C:\Windows

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

Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\9a992314512bbc93b07328b3941fe048.exe

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

controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985

C:\Windows\SysWOW64\winmm.dll Opens: C:\Windows\SysWOW64\dsound.dll C:\Windows\SysWOW64\wsock32.dll Opens: Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\winmmbase.dll Opens: C:\Windows\SysWOW64\powrprof.dll Opens: C:\Windows\SysWOW64\winnsi.dll C:\Windows\SysWOW64\gdi32.dll Opens: Opens: C:\Windows\SysWOW64\user32.dll Opens: C:\Windows\SysWOW64\msvcrt.dll

Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll

Opens: C:\Windows\SysWOW64\sspicli.dl1
Opens: C:\Windows\SysWOW64\rpcrt4.dl1
Opens: C:\Windows\SysWOW64\rpcrt4.dl1
Opens: C:\Windows\SysWOW64\combase.dl1
Opens: C:\Windows\SysWOW64\combase.dl1
Opens: C:\Windows\SysWOW64\oleaut32.dl1

C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens: Opens: C:\Windows\SysWOW64\nsi.dll Opens: C:\Windows\SysWOW64\ws2_32.dll C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\msctf.dll Opens: C:\Windows\WindowsShell.Manifest Opens: Opens: C:\Windows\SysWOW64\SHCore.dll Opens: C:\Windows\SysWOW64\profapi.dll Opens: C:\ProgramData\Remote Control PC Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\Windows\SysWOW64\dwmapi.dll

Opens: C:\Windows\Temp

Opens: C:\

C:\ProgramData\Remote Control PC\apc-host.log Opens: Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\NapiNSP.dll C:\Windows\SysWOW64\pnrpnsp.dll Opens: Opens: C:\Windows\SysWOW64\nlaapi.dll Opens: C:\Windows\SysWOW64\dnsapi.dll Opens: C:\Windows\SysWOW64\winrnr.dll Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL Opens: C:\Windows\SysWOW64\rasadhlp.dll ${\tt C:\Windows\SysWOW64\MMDevAPI.dll}$ Opens: Opens: C:\Windows\SysWOW64\cfgmgr32.dll Opens: C:\Windows\SysWOW64\devobj.dll

C:\ProgramData\Remote Control PC\hostaccount.ini Opens: Writes to: C:\ProgramData\Remote Control PC\apc-host.log Writes to: C:\ProgramData\Remote Control PC\hostaccount.ini C:\ProgramData\Remote Control PC\hoststate.dat Writes to: Reads from: C:\ProgramData\Remote Control PC\hostaccount.ini

Windows Registry Events

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

Opens key: HKLM\software\microsoft\wow64

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

Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

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

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

Opens key: HKCU\

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU\control\ panel\desktop\muicached\machinelanguageconfiguration \end{tabular}$ Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side$

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

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog

Opens kev: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

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

execution options Opens key:

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

Opens key:

HKLM\software\wow6432node\microsoft\windows

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

nt\currentversion\compatibility32

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

compatibility

Opens key:

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

Opens key: $HKLM \verb|\system| current control \verb|\sa| fips algorithm policy$

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

Opens kev:

HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration Opens key: HKLM\software\wow6432node\microsoft\ole Opens key: HKLM\software\wow6432node\microsoft\ole\tracing Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKCU\software\borland\locales HKLM\software\wow6432node\borland\locales Opens key: HKCU\software\borland\delphi\locales Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions$ Opens key: fdc1-4dc3-a9dd-070d1d495d97} Opens key: fdc1-4dc3-a9dd-070d1d495d97}\propertybag Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\profilelist Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist Opens key: $HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| \verb|\windows| current version \verb|\explorer| known folders ettings | leaves to the second of th$ Opens key: HKLM\software\policies\microsoft\sqmclient\windows Opens key: HKLM\software\microsoft\sqmclient\windows Opens key: Opens key: HKLM\software\wow6432node\microsoft\rpc Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername HKLM\system\setup Opens key: Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc Opens key: HKLM\software\policies\microsoft\windows nt\rpc Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\146b8021 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens kev: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006

HKLM\system\currentcontrolset\services\winsock\parameters
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens kev:

Opens key:

Opens key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip

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 key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient

Opens key: HKLM\software\policies\microsoft\system\dnsclient

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\}$

Opens kev:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

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

Opens key:

 $\label{local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \explorer \folder descriptions \folder \folder$

Opens key

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\defided b2f1-4857-a4ce-a8e7c6ea7d27\property bag$

Opens key

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)$

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-

1d43-42f2-9305-67de0b28fc23}\propertybag

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

 $Opens\;key: \\ \qquad \qquad \text{HKLM} software \verb|\wow6432| node \verb|\microsoft| windows | nt \verb|\currentversion| drivers 32| \\$

Opens key:

Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\render\
Opens key: HKLM\software\microsoft\windows\currentversion\mmdevices\audio\capture\
Opens key: HKLM\system\currentcontrolset\control\deviceclasses\{6994ad04-93ef-11d0-

a3cc-00a0c9223196}

Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrol\set\control\terminal server[tsuserenabled]

Queries value:

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

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

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

us[alternatecodepage]

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

 $Queries\ value: \\ HKCU \ control\ panel \ desktop \ muicached [machine preferreduil anguages]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest] \ described by the side of the sid$

Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

Queries value: HKCU\software\microsoft\windows

 $\verb|nt\currentversion\appcompatflags[showdebuginfo]| \\$

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dllnxoptions[usefilter]

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

 $\label{lem:continuous} options $$ \dim[9a992314512bbc93b07328b3941fe048.exe] $$ Queries value: $$ HKLM\software\microsoft\windows $$ nt\currentversion\gre_initialize[disablemetafiles] $$$

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[9a992314512bbc93b07328b3941fe048]
Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

 $\label{thm:linear} Queries \ value: \\ HKLM\ system\ current control set\ control\ lsa\ fips algorithm policy [enabled] \\$

Queries value: HKLM\system\currentcontrol\sa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]

Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\system\currentcontrol\set\control\wmi\security[12e1ddac-7ebb-434f-

bc58-54c27d745f8f]

Queries value: HKLM\system\currentcontrol\set\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows\error

reporting\wmr[disable]

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[category]} $$$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ [parent folder]$

Queries value:

```
fdc1-4dc3-a9dd-070d1d495d97}[description]
   Oueries value:
fdc1-4dc3-a9dd-070d1d495d97}[relativepath]
fdc1-4dc3-a9dd-070d1d495d97}[parsingname]
   Oueries value:
fdc1-4dc3-a9dd-070d1d495d97}[infotip]
   Queries value:
fdc1-4dc3-a9dd-070d1d495d97}[localizedname]
   Oueries value:
fdc1-4dc3-a9dd-070d1d495d97}[icon]
fdc1-4dc3-a9dd-070d1d495d97}[security]
fdc1-4dc3-a9dd-070d1d495d97}[streamresource]
fdc1-4dc3-a9dd-070d1d495d97}[streamresourcetype]
fdc1-4dc3-a9dd-070d1d495d97}[localredirectonly]
fdc1-4dc3-a9dd-070d1d495d97}[roamable]
fdc1-4dc3-a9dd-070d1d495d97}[precreate]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[stream]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-includescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\fo
fdc1-4dc3-a9dd-070d1d495d97}[publishexpandedpath]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[attributes]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-includescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\foldescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\fo
fdc1-4dc3-a9dd-070d1d495d97}[foldertypeid]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-
fdc1-4dc3-a9dd-070d1d495d97}[initfolderhandler]
   Oueries value:
                                          HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
   Queries value:
                                          HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:
                                          HKLM\software\microsoft\rpc[maxrpcsize]
   Oueries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
   Queries value:
                                          HKLM\system\setup[oobeinprogress]
                                          HKLM\system\setup[systemsetupinprogress]
   Oueries value:
   Queries value:
                                          HKLM\software\microsoft\rpc[idletimerwindow]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
                                          HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
   Queries value:
   Oueries value:
                                          HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog 9 [next\_catalog\_entry\_id]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]

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

Oueries value:

Queries 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] 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath] Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 000000000001 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries 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\00000000001[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\000000000002[displaystring] Queries 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\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 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\000000000002[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 00000000000003 \ [displaystring] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries 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]
- 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\000000000003[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] Queries value:
- $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ winsock 2 \ parameters \ name \ space_catalog \ services \ name \ space_catalog \ name \ name \ name \ space_catalog \ name \ n$
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 [address family] \\ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries 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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
 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\000000000005[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\0000000000005[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries 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] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries 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:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
 Queries value:

 $HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names family] \\ Queries value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[version]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]

Queries value:

 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]

 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdesc$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} \ [parent folder]$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e\} [description]$

Queries value

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\f$

Queries value:

Queries value:

 $\label{limit} \begin{tabular}{ll} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\fold$

Queries value:

 $\label{localized-hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e)\currentversion\explorer\f(8ca1)\currentversion\explorer\folderdescriptions\f(8ca1)\currentversion\explorer\folderdescriptions\f(8ca1)\currentversion\explorer\folderdescriptions\f(8ca1)\currentversion\explorer\folderdescriptions\f(8ca1)\currentversion\explorer\folderdescriptions\f(8ca1)\currentversion\explorer\explorer\folderdescriptions\f(8ca1)\currentversion\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\explorer\e$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40efa0fb-4bfc-874a-c0f2e0b9fa8e\} [icon]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\folderdescriptions\fo$

Oueries value:

a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]

a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ node \ microsoft \ windows \ node \$ a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]

a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40efa0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40efa0fb-4bfc-874a-c0f2e0b9fa8e}[stream]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ node \ microsoft \ windows \ node \$ a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]

Oueries value:

a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]

Oueries value:

 $HKLM \label{lem:hklm} White the latest and the la$ a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]

Queries value:

a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]

b2f1-4857-a4ce-a8e7c6ea7d27}[category]

b2f1-4857-a4ce-a8e7c6ea7d27}[name]

b2f1-4857-a4ce-a8e7c6ea7d27}[parentfolder]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[description]

b2f1-4857-a4ce-a8e7c6ea7d27}[relativepath]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[parsingname] Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[infotip]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[localizedname] Oueries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[icon]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[security]

b2f1-4857-a4ce-a8e7c6ea7d27}[streamresource]

b2f1-4857-a4ce-a8e7c6ea7d27}[streamresourcetype]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[localredirectonly]

b2f1-4857-a4ce-a8e7c6ea7d27}[roamable]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d65231b0b2f1-4857-a4ce-a8e7c6ea7d27}[precreate]

b2f1-4857-a4ce-a8e7c6ea7d27}[stream]

Queries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[publishexpandedpath]

Oueries value:

 $\label{local-b2} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\}[attributes]}$

Oueries value

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder b2f1-4857-a4ce-a8e7c6ea7d27\folder typeid\]$

Queries value:

 $HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} [initfolder \ handler]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\cutegory\cite{Alicentering} and the second seco$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \windows \current version \explorer \folder descriptions \folder \fold$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f38bf404-1d43-42f2-9305-67de0b28fc23\} \ [parent folder]$

Oueries value:

 $\label{thm:hklm:software} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)\f(description)$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f38bf404-1d43-42f2-9305-67de0b28fc23\}[relative path]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f38bf404-1d43-42f2-9305-67de0b28fc23\} \ [parsing name]$

Queries value:

 $\label{thm:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\cite{Continuous} in the continuous folder descriptions for the continuous folder descriptions for the continuous folder descriptions for the continuous for the continuous formula for the continuous for the continuous for the continuous for the continuous formula for the continuous for the$

Oueries value:

 $\label{thm:local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\[localized name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f38bf404-1d43-42f2-9305-67de0b28fc23\}[icon]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamresource)\f(streamr$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f38bf404-1d43-42f2-9305-67de0b28fc23\} [stream resource type]$

Queries value:

 $\label{thm:local-continuous} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \f38bf404-1d43-42f2-9305-67 de \folder \mbox{blocal redirectonly} \]$

Queries value: KI M\software\

 $\label{thm:local-hammon} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \fo$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\soft\windows\currentversion\explorer\folderdescriptions\ff38bf404-1d43-42f2-9305-67de0b28fc23\}[precreate]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f(stream)\f($

Queries value:

 $\label{lem:hklm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\[publishexpandedpath]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \color= \co$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(f38bf404-1d43-42f2-9305-67de0b28fc23)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldertypeid)\f(foldert$

Queries value:

 $\label{thm:hklm} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \f38bf404-1d43-42f2-9305-67 de0 b28fc23 \[initfolder handler]$

Oueries value: HKLM\system\currentcontrolset\control\samservicelist[samservicelist]

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

nt\currentversion\drivers32[wave]

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

nt\currentversion\drivers32[wave1]

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

nt\currentversion\drivers32[wave2]

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

nt\currentversion\drivers32[wave3]

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

nt\currentversion\drivers32[wave4]

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

nt\currentversion\drivers32[wave5]

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

nt\currentversion\drivers32[wave6]

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

nt\currentversion\drivers32[wave7]

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

nt\currentversion\drivers32[wave8]

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

nt\currentversion\drivers32[wave9]

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

nt\currentversion\drivers32[midi]

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

nt\currentversion\drivers32[midi1]

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

nt\currentversion\drivers32[midi2]

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

 $\verb|nt\currentversion\drivers32[midi3]|\\$

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

nt\currentversion\drivers32[midi4]

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

nt\currentversion\drivers32[midi5]

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

nt\currentversion\drivers32[midi6]

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

nt\currentversion\drivers32[midi7]

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

nt\currentversion\drivers32[midi8]

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

nt\currentversion\drivers32[midi9]

Queries value: