Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 192, Task ID: 766

Task ID: 766 Risk Level: 1

Date Processed: 2016-04-28 13:08:28 (UTC)

Processing Time: 61.24 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\315ab636e84b1f5697cf0a35f5f0899d.exe"

Sample ID: 192 Type: basic Owner: admin

Label: 315ab636e84b1f5697cf0a35f5f0899d

Date Added: 2016-04-28 12:45:10 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gu File Size: 524288 bytes

MD5: 315ab636e84b1f5697cf0a35f5f0899d

SHA256: 72ae0cd9d65f7fcf02401bca471a7dfc3b3648bb83b5b186fe00dd8f7a876787

Description: None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\315ab636e84b1f5697cf0a35f5f0899d.exe

["C:\windows\temp\315ab636e84b1f5697cf0a35f5f0899d.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Creates: C:\Windows\SysWOW64\log.txt

Opens: C:\Windows\Prefetch\315AB636E84B1F5697CF0A35F5F08-6F4FA641.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64

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

Opens: C:\Windows\Temp\315ab636e84b1f5697cf0a35f5f0899d.exe

Opens: C:\Windows\SysWOW64\ntdll.dll Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\KernelBase.dll Opens: Opens: C:\Windows\apppatch\sysmain.sdb Opens: C:\Windows\SysWOW64\winmm.dll C:\Windows\SysWOW64\mfc42.dll Opens: Opens: C:\Windows\SysWOW64\wsock32.dll Opens: C:\Windows\SysWOW64\winmmbase.dll C:\Windows\SysWOW64\odbc32.dll Opens: Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\Windows\SysWOW64\combase.dll Opens: C:\Windows\SysWOW64\msvcrt.dll Opens: C:\Windows\SysWOW64\gdi32.dll Opens: C:\Windows\SysWOW64\user32.dll

C:\Windows\SysWOW64\bcryptprimitives.dll Opens: Opens: C:\Windows\SysWOW64\cryptbase.dll Opens: C:\Windows\SysWOW64\sspicli.dll C:\Windows\SysWOW64\rpcrt4.dll Opens: Opens: C:\Windows\SysWOW64\ole32.dll Opens: C:\Windows\SysWOW64\oleaut32.dll C:\Windows\SysWOW64\advapi32.dll Opens: Opens: C:\Windows\SysWOW64\shlwapi.dll Opens: C:\Windows\SysWOW64\shell32.dll C:\Windows\SysWOW64\nsi.dll Opens: Opens: C:\Windows\SysWOW64\ws2_32.dll C:\Windows\SysWOW64\imm32.dll Opens:

Opens: C:\Windows\SysWOW64\en-US\MFC42.dll.mui

Opens: C:\Windows\Temp

Opens:

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

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

C:\Windows\SysWOW64\msctf.dll

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

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

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

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

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

Opens: C:\Windows\SysWOW64\winrnr.dll
Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens: C:\Windows\SysWOW64\winnsi.dll
Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL
Opens: C:\Windows\SysWOW64\rasadhlp.dll
Reads from: C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Creates key: HKCR\orangewebserver.document

Creates key: HKCR\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}

Creates key: HKCR\orangewebserver.document\clsid

Creates key: HKCR\www6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}\progid

Creates key: HKCR\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-

b29c6464d35e}\inprochandler32

Creates key: HKCR\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-

b29c6464d35e}\localserver32

Creates key: HKCU\software\orange\config

Creates key: HKCU\software

Creates key: HKCU\software\orange

Creates key: HKCR\or\lic
Creates key: HKCR\or
Creates key: HKCR\or\inst

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

Creates key: HKCU\software\orange\dynamic
Opens key: HKLM\software\microsoft\wow64

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

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

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

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

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

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

Opens key: HKCU\

Opens key: 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\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags

 $\label{lem:condition} Opens \ key: \\ HKLM \ software \ microsoft \ windows \\ nt \ current version \ approximately a flags \ disable 8 and 16 bit mitigation \\$

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

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

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32

Opens key:

compatibility
Opens key: HKLMN

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

HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

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

Opens key: ${\tt HKLM \ } {\tt System \ } {\tt current control \ } {\tt lsa}$

Opens key:

 $\label{thm:linear_ham} \begin{tabular}{ll} HKLM \end{tabular} is supposed that the linear control of the lin$

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: HKLM\software\wow6432node\microsoft\bidinterface\loader

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

Opens key: $\label{lem:hklmsoftwarepoliciesmicrosoftsqmclientwindows} \label{lem:hklmsoftwarepoliciesmicrosoftsqmclientwindows}$

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

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

Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\wow6432node\clsid
Opens key: HKCU\software\classes\orangewebserver.document

Opens key: HKCR\orangewebserver.document

Opens key: HKLM\software\classes
Opens key: HKCU\software\classes\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}
Opens key: HKCR\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}
Opens key: HKCU\software\classes\orangewebserver.document\clsid
Opens key: HKCU\software\classes\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-

b29c6464d35e}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-

b29c6464d35e}\localserver32

Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKLM\system\currentcontrolset\control\nls\locale

Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback

 $Opens \ key: \\ HKLM\software\microsoft\windows \\ nt\currentversion\languagepack\surrogatefallback\segoe \ ui \\$

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions$

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-

a0fb-4bfc-874a-c0f2e0b9fa8e}

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{7c5a40effolder \ and \ baselines \ and \ and \ baselines \ and \ and$

a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag

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

Opens key

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ (d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d65231b0-d$

b2f1-4857-a4ce-a8e7c6ea7d27}

Opens key:

b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag

Opens key

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

1d43-42f2-9305-67de0b28fc23}

Opens key

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf404-f38bf40$

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

Opens key:

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

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

 $\begin{tabular}{lll} Opens~key: & HKCU\software\classes\or\lic\\ Opens~key: & HKCU\software\classes\or\linst\\ \end{tabular}$

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

 $Opens\ key: \\ HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ appid_catalog$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\0cb89224

Opens key:

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

Opens key:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol_catalog 9 \setminus 00000005$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010
Opens key:

Opens key:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
 Opens key:
                          HKLM\software\wow6432node\microsoft\rpc
                          HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens kev:
 Opens key:
                          HKLM\system\setup
 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\dnscache\parameters
 Opens key:
                          HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
 Opens kev:
                          HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key:
                          HKLM \verb|\software\\| wow 6432 node\\| policies\\| microsoft\\| system\\| dnsclient
 Opens key:
                          HKLM\software\policies\microsoft\system\dnsclient
 Opens key:
                          HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key:
                          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key:
                          HKLM\system\currentcontrolset\services\winsock\setup migration\providers
 Opens kev:
                          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
 Queries value:
                          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value:
                          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                          HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                          HKCU\control panel\desktop[preferreduilanguages]
 Oueries value:
 Queries value:
                          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Oueries value:
                          HKCU\software\microsoft\windows
 Queries value:
nt\currentversion\appcompatflags[showdebuginfo]
 Queries value:
                          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Oueries value:
options\dllnxoptions[usefilter]
                          HKLM\software\microsoft\windows nt\currentversion\image file execution
 Oueries value:
options\dllnxoptions[315ab636e84b1f5697cf0a35f5f0899d.exe]
 Queries value:
                          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Oueries value:
                          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[315ab636e84b1f5697cf0a35f5f0899d]
                          HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\windows[loadappinit_dlls]
                          HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
 Queries value:
                          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Oueries value:
                          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                          HKLM\software\microsoft\ole[aggressivemtatesting]
 Queries value:
 Queries value:
                          HKLM\software\wow6432node\microsoft\bidinterface\loader[:ldrmsg]
 Oueries value:
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus bid \\ interface \setminus loader \\ [c:\windows \setminus temp \setminus 315 \\ ab \\ 636e84b \\ 1f5697cf0 \\ a35f5f0 \\ 899d.exe: \\ 2792]
 Queries value:
HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus bidinterface \setminus loader[c:\windows \setminus temp \setminus 315ab 636e 84b 1f 5697cf 0a 35f 5f 0899d.exe]
 Queries value:
HKLM\software\wow6432node\microsoft\bidinterface\loader[c:\windows\temp\*1
                          HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| bidinterface\\| loader[:path]|
 Queries value:
                          HKLM\system\currentcontrolset\control\wmi\security[f34765f6-a1be-4b9d-
 Oueries value:
1400-b8a12921f7041
                          HKLM\software\wow6432node\microsoft\windows\windows error
 Queries value:
reporting\wmr[disable]
 Oueries value:
                          HKLM\software\microsoft\ole[maximumallowedallocationsize]
 Queries value:
                          HKLM\software\microsoft\sqmclient\windows[ceipenable]
                          {\it HKLM \ } system \ `current control set \ `control \ `session' \\
 Oueries value:
manager[safeprocesssearchmode]
 Oueries value:
                          HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
 Queries value:
                          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Oueries value:
                          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
```

HKLM\system\currentcontrolset\control\nls\locale[00000409]

Queries value:

```
Oueries value:
                                                                  HKLM\system\currentcontrolset\control\nls\language groups[1]
                                                                  HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
    Queries value:
                                                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
    Queries value:
                                                                  HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
    Oueries value:
                                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                                                                  HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                                                                  HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
                                                                 HKLM\software\microsoft\windows
    Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
                                                                  HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                                                                 HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
    Queries value:
                                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
                                                                  HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
                                                                  HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
    Queries value:
                                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
                                                                  HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                                                                 HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
    Queries value:
                                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                                                                  HKLM\software\microsoft\windows
    Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
    Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
    Oueries value:
HKLM \label{lem:hklm} White the latest and the la
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
    Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
    Queries value:
HKLM \label{lem:hklm} White the latest and the la
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
    Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
    Queries value:
HKLM \label{lem:hklm} White the latest and the la
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
    Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
    Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
    Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
    Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
    Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{7c5a40effolder \ and \ baselines \ and \ and \ baselines \ and \ and
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
    Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
    Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
    Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
```

Queries value:

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

Oueries value:

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

Oueries 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:

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

Oueries value

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

Oueries value:

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

Queries value: HKLM\system\currentcontrol\s\sorting\ids[en-us] Queries value: HKLM\system\currentcontrol\st\control\nls\sorting\ids[en]

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In the constant of the$

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} \ [parsing name]$

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} \ [localized name]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} I icon \end{array} Licon \end{array} Licon \end{array} Hklm \end{array} Licon \end{$

Queries value:

 $\label{local-hklm} HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} [security]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\} [stream resource]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In construction \explorer \end{array} In construction \end{array} The label{lem:hklmsoftware} The label{lem:hklmsof$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{array} In the constraint of the cons$

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\}[stream]$

Queries value:

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

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{d65231b0-b2f1-4857-a4ce-a8e7c6ea7d27\}[foldertypeid]$

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f38bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f18bf404-f$

```
1d43-42f2-9305-67de0b28fc23}[name]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[parentfolder]
    Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f38bf404-fine \ folder \ f
1d43-42f2-9305-67de0b28fc23}[description]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[relativepath]
    Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f38bf404-fine \ folder \ f
1d43-42f2-9305-67de0b28fc23}[parsingname]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[infotip]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[localizedname]
    Queries value:
1d43-42f2-9305-67de0b28fc23}[icon]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[security]
    Queries value:
1d43-42f2-9305-67de0b28fc23}[streamresource]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[streamresourcetype]
    Queries value:
1d43-42f2-9305-67de0b28fc23}[localredirectonly]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[roamable]
    Oueries value:
1d43-42f2-9305-67de0b28fc23}[precreate]
    Oueries value:
```

 $\label{thm:local-ham} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \f138 bf404-1d43-42f2-9305-67 de0 b28 fc23 \fixed \cite{Constraints} \cite{Constraints} \fixed \cite{Constraints} \cite$

Queries value:

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

Queries value:

Queries value:

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

Queries value:

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

Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]

Queries value: HKCU\software\orange\config[minimize]

Queries value: HKCR\or\lic[key]
Queries value: HKCR\or\inst[timestamp]

Queries value:

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

Queries value:

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

Oueries value:

Queries value

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]

Queries value:

Queries 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] Queries value:

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

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]
 Queries value:

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

Oueries 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] 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\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 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]
 Queries 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\000000000001[storesserviceclassinfo]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[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]
 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]
 Oueries 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\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000003 \ [address family] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000003 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerinfo]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000004 [library path] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_lember \namespace_le$
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \catalog_entries \catalog \catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 0000000000004 [storesservice class info] \ Oueries \ value:$
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath] Queries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring] Oueries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000005 \ [providerid] \ Oueries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\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\000000000005[version]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo] Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$

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

 $HKLM \system \current control set \services \winsock 2 \parameters \names pace_catalog 5 \catalog_entries \names \names$

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

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

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

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

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

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

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

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws2_32 numbandle buckets]$

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

Queries value:

 $\label{lem:hklm} \verb+Kklm/system/currentcontrolset/control/computername active computername [computername]$

 Queries value:
 HKLM\system\setup[oobeinprogress]

 Queries value:
 HKLM\system\setup[systemsetupinprogress]

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

 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:
 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]

Queries value:

Queries value:

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

Queries value:

Queries value: HKCU\software\orange\dynamic[url]
Queries value: HKCU\software\orange\dynamic[folder]
Queries value: HKCU\software\orange\dynamic[filename]
Queries value: HKCU\software\orange\dynamic[username]
Queries value: HKCU\software\orange\dynamic[password]
Queries value: HKCU\software\orange\dynamic[flag]
Sets/Creates value: HKCR\orangewebserver.document[]

Sets/Creates value: HKCR\www6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}[]

Sets/Creates value: HKCR\orangewebserver.document\clsid[]

Sets/Creates value: HKCR\www6432node\clsid\{915b9b42-85bd-11d4-bd1f-b29c6464d35e}\progid[]

Sets/Creates value: HKCR\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-

b29c6464d35e}\inprochandler32[]

Sets/Creates value: HKCR\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-

b29c6464d35e}\localserver32[]

Sets/Creates value: HKCU\software\orange\config[rootdir]
Sets/Creates value: HKCU\software\orange\config[minimize]
Sets/Creates value: HKCU\software\orange\config[port]
Sets/Creates value: HKCU\software\orange\config[addrstyle]

Sets/Creates value: HKCR\or\inst[timestamp]