# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 192, Task ID: 769

Task ID: 769 Risk Level: 1

Date Processed: 2016-04-28 13:08:38 (UTC)

Processing Time: 61.32 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 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

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX

Creates event: \BaseNamedObjects\BFE\_Notify\_Event\_{ff21d539-19b5-4581-ac7a-

5084e25b99bd}

#### File System Events

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

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

Opens: C:\Windows

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

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

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

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

Opens: C:\Windows\SysWOW64 Opens: C:\windows\temp\WINMM.dll C:\Windows\SysWOW64\winmm.dll Opens: Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\windows\temp\MFC42.DLL Opens: C:\Windows\SysWOW64\mfc42.dll Opens: C:\windows\temp\ODBC32.dll Opens: C:\Windows\SysWOW64\odbc32.dll C:\windows\temp\WSOCK32.dll Opens: Opens: C:\Windows\SysWOW64\wsock32.dll Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\odbcint.dll Opens:

Opens: C:\Windows\SysWOW64\en-US\odbcint.dll.mui
Opens: C:\Windows\SysWOW64\en-US\MFC42.dll.mui
Opens: C:\Windows\SysWOW64\MFC42LOC.DLL
Opens: C:\Windows\SysWOW64\MFC42LOC.DLL.DLL
Opens: C:\Windows\System32\MFC42LOC.DLL

Opens: C:\Windows\Temp

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

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

Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\Fonts\StaticCache.dat

Opens: C:\

Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui

C:\Windows\SysWOW64\dnsapi.dll Opens: Opens: C:\Windows\SysWOW64\winrnr.dll C:\windows\temp\IPHLPAPI.DLL Opens: Opens: C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: C:\windows\temp\WINNSI.DLL Opens: C:\Windows\SysWOW64\winnsi.dll Opens: C:\windows\temp\dhcpcsvc6.DLL C:\Windows\SysWOW64\dhcpcsvc6.dll Opens: C:\windows\temp\dhcpcsvc.DLL Opens: Opens: C:\Windows\SysWOW64\dhcpcsvc.dll Opens: C:\Windows\SysWOW64\FWPUCLNT.DLL Opens: C:\windows\temp\rasadhlp.dll Opens: C:\Windows\SysWOW64\rasadhlp.dll C:\Windows\SysWOW64\WSHTCPIP.DLL Opens: Reads from: C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

Creates key: HKCR\orangewebserver.document

Creates key:  $HKCR \setminus wow6432 node \setminus clsid \setminus \{915b9b42 - 85bd - 11d4 - bd1f - b29c6464d35e\}$ 

Creates key: HKCR\orangewebserver.document\clsid

Creates key:

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

b29c6464d35e}\inprochandler32

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

b29c6464d35e}\localserver32

Creates key: HKCU\software\orange\config

Creates key: HKCU\software HKCU\software\orange Creates key:

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

 $\label{lem:hklm} \verb+Kklm \+ system \+ current control set \+ services \+ tcpip \+ parameters$ Creates key:

Creates key: HKCU\software\orange\dynamic

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

options

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

Opens key: HKLM\software\microsoft\wow64

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

execution options

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

Opens key:

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

Opens key:  $HKLM \setminus software \setminus policies \setminus microsoft \setminus windows \setminus safer \setminus code identifiers$ 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

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

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration Opens kev:

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

Opens key:  ${\tt HKCU \backslash control\ panel \backslash desktop}$ 

Opens key: HKCU\control panel\desktop\muicached

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

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

Opens key:

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

nt\currentversion\diagnostics

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

nt\currentversion\gre\_initialize

HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32

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

Opens key:

compatibility

Opens key:

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

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

Opens key: HKLM\software\wow6432node\microsoft\oleaut HKLM\software\wow6432node\microsoft\bidinterface\loader Opens key:

Opens key: HKLM\system\currentcontrolset\control\cmf\config Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr

HKCU\software\odbc\odbc.ini\odbc Opens key:

Opens key: HKLM\software\wow6432node\odbc\odbc.ini\odbc

HKCU\software\classes\ Opens kev:

```
Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid
     Opens key:
                                                                        HKCU\software\classes\orangewebserver.document
     Opens key:
                                                                        HKCR\orangewebserver.document
     Opens key:
                                                                        HKLM\software\classes
                                                                        HKCU\software\classes\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-
     Opens kev:
b29c6464d35e}
                                                                        HKCR \setminus wow6432 node \setminus clsid \setminus \{915b9b42 - 85bd - 11d4 - bd1f - b29c6464d35e\}
     Opens key:
                                                                        HKCU\software\classes\orangewebserver.document\clsid
     Opens key:
     Opens key:
                                                                        HKCU\software\classes\wow6432node\clsid\{915b9b42-85bd-11d4-bd1f-
b29c6464d35e}\progid
     Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{915b9b42 - 85bd - 11d4 - bd1f - 11d4 - bd1f - 11d4 - bd1f - 11d4 - 11d4
b29c6464d35e}\inprochandler32
    Opens key:
                                                                       HKCU \setminus software \setminus classes \setminus wow6432 \\ node \setminus clsid \setminus \{915b9b42-85bd-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1f-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-bd1-11d4-
 b29c6464d35e}\localserver32
     Opens key:
                                                                       HKLM\system\currentcontrolset\control\nls\extendedlocale
     Opens key:
                                                                        HKLM\system\currentcontrolset\control\nls\locale
     Opens kev:
                                                                       HKLM\svstem\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
                                                                       HKLM\software\microsoft\windows
     Opens key:
nt\currentversion\languagepack\datastore_v1.0
                                                                       HKLM\software\microsoft\windows
     Opens key:
\verb|nt\current| version \verb|\language| pack \verb|\surrogatefall| back |
                                                                       HKLM\software\microsoft\windows
     Opens key:
nt\currentversion\languagepack\surrogatefallback\segoe ui
     Opens key:
Opens key:
a0fb-4bfc-874a-c0f2e0b9fa8e}
    Opens kev:
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\windows\currentversion
     Opens key:
HKLM \label{lem:hklm} White the latest and the la
b2f1-4857-a4ce-a8e7c6ea7d27}
     Opens key:
b2f1-4857-a4ce-a8e7c6ea7d27}\propertybag
     Opens key:
1d43-42f2-9305-67de0b28fc23}
     Opens key:
1d43-42f2-9305-67de0b28fc23}\propertybag
     Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\315ab636e84b1f5697cf0a35f5f0899d.exe
                                                                       HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
    Opens kev:
 Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
                                                                       HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
     Opens kev:
Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
     Opens key:
                                                                       HKLM\software\wow6432node\microsoft\ctf\
                                                                        HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus known classes
     Opens key:
                                                                       HKCU\software\classes\or\lic
     Opens key:
     Opens key:
                                                                       HKCU\software\classes\or\inst
     Opens key:
                                                                       HKLM\software\policies\microsoft\sqmclient\windows
     Opens key:
                                                                       HKLM\software\microsoft\samclient\windows
                                                                       HKLM\system\currentcontrolset\services\winsock2\parameters
     Opens key:
     Opens key:
                                                                       HKLM\system\currentcontrolset\services\winsock2\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\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
    Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000
    Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
     Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006 Opens key: 

Opens key:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000005

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
   Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 000000000011) \ (catalog\_entries \ (catalog \ (catalog\_entries \ (catalog \ (catal
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
   Opens key:
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:
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\000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
   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
                                             HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens key:
   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\system\currentcontrolset\control\sqmservicelist
   Opens key:
                                             HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
   Opens key:
                                             HKLM\system\currentcontrolset\services\dns
   Opens key:
                                             HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
                                             HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens key:
   Opens key:
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
                                             HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens kev:
   Opens key:
e1e01c1f69b5}
  Opens kev:
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
  Opens kev:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
   Opens key:
                                             HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens key:
                                             HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:
                                             \label{lem:hklm} \verb+Kklm \system \current control set \services \tcpip6 \parameters \winsock
   Opens key:
                                             HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:
                                             HKLM\system\currentcontrolset\services\winsock\setup migration\providers
                                             HKLM\system\currentcontrolset\services\winsock\setup
   Opens key:
migration\providers\tcpip
                                             \label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current version + image + file + execution + image + file + image +
   Queries value:
options[disableusermodecallbackfilter]
                                             HKLM\svstem\currentcontrolset\control\session
   Oueries value:
manager[cwdillegalindllsearch]
                                             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
   Oueries value:
   Oueries 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:
   Oueries value:
                                             HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
   Oueries value:
                                             HKCU\control panel\desktop[preferreduilanguages]
```

HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Queries value:

```
Oueries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                                 HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
   Oueries value:
                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[315ab636e84b1f5697cf0a35f5f0899d]
   Oueries value:
                                                 HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
   Oueries value:
                                                 HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:
                                                 HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\cmf\config[system]
   Oueries value:
                                                 HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
   Queries value:
                                                 HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:
                                                 HKLM\svstem\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
                                                 HKLM\software\microsoft\windows
   Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
                                                 HKLM\software\microsoft\windows
   Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane1]|
                                                 HKLM\software\microsoft\windows
   Oueries value:
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]
   Oueries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
   Oueries value:
                                                 HKLM\software\microsoft\windows
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
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
                                                 HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
   Queries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
   Oueries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
   Oueries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
   Queries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                                                 HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
   Oueries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
   Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
   Oueries value:
HKLM \label{lem:hklm} White the latest and the la
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
   Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
   Oueries value:
HKLM \label{lem:hklm} White the latest and the la
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
   Oueries value:
```

Queries value:

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

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

Queries value:

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

Oueries value:

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

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]

Oueries value:

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

Oueries value:

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

Oueries value:

 $\label{local-operator} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]$ 

Oueries value:

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

Queries value:

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

Queries value

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

Oueries value

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

Queries value

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

Oueries value

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

Oueries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{local-b2} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder descriptions\folder description\folder description\folder\f$ 

Queries value:

Queries value:

Queries value:

Queries value:

 $\label{lem:hklmsoftwarewow6432node} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds \folds\$ 

Queries value:

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder\fol$ 

Queries value:

Queries value:

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[stream]

Oueries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[publishexpandedpath]

b2f1-4857-a4ce-a8e7c6ea7d27}[attributes]

Oueries value:

b2f1-4857-a4ce-a8e7c6ea7d27}[foldertypeid]

b2f1-4857-a4ce-a8e7c6ea7d27}[initfolderhandler]

1d43-42f2-9305-67de0b28fc23}[category]

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

1d43-42f2-9305-67de0b28fc23}[parentfolder]

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

1d43-42f2-9305-67de0b28fc23}[relativepath]

1d43-42f2-9305-67de0b28fc23}[parsingname]

1d43-42f2-9305-67de0b28fc23}[infotip]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[localizedname]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f38bf404-f1842\} \\ f38bf404-f1842 \\ f38bf404$ 1d43-42f2-9305-67de0b28fc23}[icon]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[security]

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{f38bf404-f1842\} \\ f38bf404-f1842 \\ f38bf404$ 1d43-42f2-9305-67de0b28fc23}[streamresource]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[streamresourcetype]

Oueries value:

HKLM\software\www6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[localredirectonly]

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f38bf404-f18bf404$ 1d43-42f2-9305-67de0b28fc23}[roamable]

Oueries value:

1d43-42f2-9305-67de0b28fc23}[precreate]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[stream]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[publishexpandedpath]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[attributes]

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[foldertypeid]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[initfolderhandler]

Queries value: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]

Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext] Queries value: HKCU\software\orange\config[minimize]

Oueries value: HKCR\or\lic[kev] Queries value: HKCR\or\inst[timestamp]

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

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[winsock\_registry\_version]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[namespace\_callout]

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[serial\_access\_num]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[next\_catalog\_entry\_id]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9[num\_catalog\_entries]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000001[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\0000000000002[packedcatalogitem] Oueries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000004[packedcatalogitem]
 Oueries 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]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000008[packedcatalogitem] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000009 \ [packed catalog item] \ Queries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[packedcatalogitem] Queries 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]

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

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

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

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]
Queries value:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storesserviceclassinfo]
 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\00000000002[librarypath] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[displaystring]
Oueries value:

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

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog5 \ catalog\_entries \ 00000000000002 [storesservice class info] \ Queries \ value:$ 

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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[displaystring] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerid]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[enabled]
 Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$ 

```
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace\_catalog 5 \ catalog\_entries \ 000000000003 \ [storesservice class in fo] \ Queries \ value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[supportednamespace]
Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ catalog\_entries \ 00000000000004 \ [enabled] \ Oueries \ value:$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[version] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[librarypath]
Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace\_catalog5 \catalog\_entries \0000000000005 \[displaystring] \queries \value:$ 

 $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace\_catalog \catalog\_entries \namespace\_catalog \catalog\_entries \catalog \catalog\_entries \catalog \catalog\_entries \catalog \cat$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
Queries 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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[librarypath] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring]
 Oueries value:

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\00000000006[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storesserviceclassinfo]
 Oueries 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\software\microsoft\rpc[maxrpcsize]
Oueries value:

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

Queries value: HKLM\system\setup[oobeinprogress]

Queries value:HKLM\system\setup[systemsetupinprogress]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]Queries value:HKLM\system\currentcontrolset\services\tcpip\parameters[domain]Queries value:HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
 Oueries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Oueries value:

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

HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
 Oueries value:

 $\label{local-problem} \mbox{\tt HKLM} \mbox{\tt system} \mbox{\tt current} \mbox{\tt controlset} \mbox{\tt services} \mbox{\tt tcpip} \mbox{\tt parameters} \mbox{\tt [prioritizerecorddata]}$ 

Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: Oueries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] Queries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl] Queries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value:  $\label{lem:hklm} \verb+Kklm \ system \ current control set \ \verb+services \ \verb+tcpip \ parameters [maxnumber of addresses to register]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [update to plevel domain zones]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [enable multicast]$ Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags] Queries value:  $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicasts endermax time out]$ Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration] Queries value: Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts] Queries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[searchlist] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[enabledhcp] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[registrationenabled] Queries value: e1e01c1f69b5}[registeradaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[domain] Queries value: e1e01c1f69b5}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpv6domain] Queries value: e1e01c1f69b5}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[dhcpnameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp] Oueries value: 806e6f6e6963}[registrationenabled] Queries value: 806e6f6e6963}[registeradaptername] Oueries value: 806e6f6e6963}[domain] Queries value: 806e6f6e6963}[dhcpdomain] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver] HKLM\system\currentcontrolset\services\tcpip\linkage[bind] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165e1e01c1f69b5}[disableadapterdomainname] Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration maxaddress count]$ 

Oueries value:

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enablemulticast]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [query adapter name]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '{846ee342-7039-11de-9d20-806e6f6e6963} \ [disable adapter domain name]$ 

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate]

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable adapter domain name registration]$ 

Oueries value:

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [maxnumber of addresses to register]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \end{4.846} ea 342-7039-11 de-9 d20-806 e6 f6 e6 963 \end{4.846} enable multicast \end{4.846}$ 

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdl1]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

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:

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

Queries value:

Queries value:

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} winsock [used elayed acceptance] \\$ 

Queries value:

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

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\wow6432node\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]