Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 626, Task ID: 2451

Task ID: 2451 Risk Level: 6

Date Processed: 2016-02-22 05:31:51 (UTC)

Processing Time: 6.52 seconds
Virtual Environment: IntelliVM

Execution Arguments:

"c:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"

Sample ID: 626 Type: basic Owner: admin

Label: b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5

Date Added: 2016-02-22 05:26:50 (UTC)

File Type: PE32:win32:gui File Size: 393212 bytes

MD5: ba04839db97a1b934cd9e470795ccf51

SHA256: b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5

Description: None

Pattern Matching Results

4 Reads process memory

- 5 Abnormal sleep detected
- 5 Possible injector
- 6 Tries to detect VM environment

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process:

C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe

 $\hbox{ ["C:\windows\setminus temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"] } \\$

Reads from process: PID:1104 C:\Windows\explorer.exe

Terminates process:

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\276188B23DF42F38

Creates mutex: \Sessions\1\BaseNamedObjects\AE2F39DFEE6EA723

File System Events

Opens: C:\Windows\Prefetch\B3AF5BCCF7891B0251AAA73F063F1-4CD469AF.pf

Opens.
C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.ENU

 $Opens: \\ C: \windows \texttt{\temp} b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.ENU.DLL \\ DLL \windows \texttt{\temp} b3af5bccf7891b0251aaaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.ENU.DLL \\ DLL \windows \texttt{\temp} b3af5bccf7891b0251aaaa73f063f1d9e5e72d1433a46451aaaa73f063f1d9e5e72$

Opens: C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.EN

C:\windows\temp\b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.EN.DLL

 $Opens: \\ C: \Windows \Globalization \SortIng \SortDefault.nls$

Opens: C:\Windows\System32\Wbem\VBoxHook.dll

Opens: C:\Windows\System32\WindowsPowerShell\v1.0\VBoxHook.dll

Opens: C:\WINDOWS\system32\drivers\VBoxMouse.sys
Opens: C:\WINDOWS\system32\drivers\vmmouse.sys
Opens: C:\WINDOWS\system32\drivers\vmhgfs.sys

C:\WINDOWS\system32\drivers\vpc-s3.sys Opens: C:\WINDOWS\system32\drivers\vpcubus.sys Opens:

Opens: C:\Users\Admin\AppData\Roaming Opens: C:\Users\Admin\AppData\Local Opens: C:\windows\temp\profapi.dll Opens: C:\Windows\System32\profapi.dll

Opens: C:\ProgramData C:\Users\Admin Opens:

Windows Registry Events

Creates key: HKCU\software\microsoft\internet explorer\main\featurecontrol

Creates key: HKCU\software\microsoft\internet explorer\international

Creates key: HKCU\software\d0ddaac5a9 HKLM\software\d0ddaac5a9 Creates key:

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

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

Opens key: HKCU\

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

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

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

HKCU\control panel\desktop Opens key:

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside Opens kev: HKLM\svstem\currentcontrolset\control\nls\sorting\versions Opens key: HKLM\system\currentcontrolset\control\error message instrument\ Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre_initialize$ Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

HKI M\ Opens kev:

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

Opens kev: HKLM\software\microsoft\ole Opens key: HKLM\software\microsoft\ole\tracing Opens key: HKLM\software\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\services\crypt32

Opens key: HKLM\software\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet

settings

Opens key: HKCU\software\borland\locales Opens key: HKCU\software\borland\delphi\locales

HKLM\system\currentcontrolset\control\nls\customlocale Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\policies\microsoft\sqmclient\windows

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

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

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\31f8160b

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019

Opens key:

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

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

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

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Onens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
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 kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000

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

Opens key: HKU\

Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet settings\zones\1

Opens key: HKCU\software\

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

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

Opens key: HKLM\system\setup

Opens key: HKLM\hardware\devicemap\scsi\scsi port 0\scsi bus 0\target id 0\logical

unit id 0

HKLM\hardware\description\system Opens kev: HKLM\system\currentcontrolset\services\disk\enum Opens key: Opens key: HKLM\software\oracle\virtualbox guest additions Opens key: HKLM\software\vmware, inc.\vmware tools Opens key: $\label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows\+ current version\+ app\ paths\+ wireshark.exe$ Opens key: HKLM\software\ HKLM\software\d0ddaac5a9\ Opens kev: Opens key: HKCU\software\d0ddaac5a9\

Opens key: HKCU\software\microsoft\windows\currentversion\app paths\wireshark.exe
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\wireshark
Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\wireshark

Opens key: HKLM\software\wireshark
Opens key: HKCU\software\wireshark

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\fiddler.exe
Opens key: HKCU\software\microsoft\windows\currentversion\app paths\fiddler.exe
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\fiddler2.exe
Opens key: HKCU\software\microsoft\windows\currentversion\app paths\fiddler2.exe
Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\fiddler2
Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\fiddler2

Opens key: HKLM\software\microsoft\fiddler2
Opens key: HKCU\software\microsoft\fiddler2

Opens key: HKCR\software\ieinspectorsoft\httpanalyzeraddon

Opens key: HKCU\software\classes\software\ieinspectorsoft\httpanalyzeraddon

Opens key: HKCR\iehttpanalyzer.httpanalyzeraddon

Opens key: HKCU\software\classes\iehttpanalyzer.httpanalyzeraddon

Opens key: HKCR\httpanalyzerstd.httpanalyzerstandalone

 $Opens~key: \\ HKCU \setminus software \setminus classes \setminus httpanalyzerstd.httpanalyzerstandalone$

Opens key: HKCR\charles.amf.document

Opens key: HKCU\software\classes\charles.amf.document

Opens key: HKCR\charles.document

Opens key: HKCU\software\classes\charles.document

Opens key: HKLM\software\xk72 ltd folder
Opens key: HKCU\software\xk72 ltd folder
Opens key: HKLM\software\microsoft\rpc

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

Opens key:

 $\label{thm:local_hammon} \begin{tabular}{ll} HKLM \end{tabular} so ftwo explorer \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular} and \end{tabular} in the constant \end{tabular} and \end{tabular}$

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

```
a03a-e3ef65729f3d}\propertybag
   Opens key:
                                             HKCU\software\microsoft\windows\currentversion\explorer
   Opens key:
                                             HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
   Opens kev:
Opens key:
                                             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens kev:
9d55-7b8e7f157091}
  Opens key:
9d55-7b8e7f157091}\propertybag
   Opens key:
a9dd-070d1d495d97}
   Opens key:
HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ \ folder descriptions \ \ \ \{62ab5d82-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-4dc3-fdc1-
a9dd-070d1d495d97}\propertybag
                                            HKLM\software\microsoft\windows nt\currentversion\profilelist
   Opens kev:
   Opens key:
HKLM \ software \ `microsoft \ 'windows \ 'current version' \ explorer \ 'folder descriptions \ '\xi 5e6c858f-0e22-4760-1200' \ descriptions \ 'folder descriptions' \ (folder descriptions) \ (folde 
9afe-ea3317b67173}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
                                             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
                                             HKLM\software\microsoft\windows\currentversion\run
   Opens key:
   Queries value:
                                             HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
                                             HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
   Queries value:
   Oueries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
                                             HKCU\control panel\desktop[preferreduilanguages]
                                             HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
   Queries value:
   Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]
   Oueries value:
                                             HKLM\svstem\currentcontrolset\control\nls\sorting\versions[]
   Oueries value:
                                             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
                                             HKLM\software\microsoft\windows
   Oueries value:
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:
                                            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5]
                                            HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\windows[loadappinit_dlls]
                                            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Oueries value:
   Oueries value:
                                             HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:
                                             HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                                             HKLM\software\microsoft\windows\currentversion\internet
   Queries value:
settings[disableimprovedzonecheck]
   Queries value:
                                             HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
                                             HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
   Queries value:
                                             HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                                             HKLM\software\microsoft\sqmclient\windows[ceipenable]
   Queries value:
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
HKLM\svstem\currentcontrolset\services\winsock2\parameters[namespace callout]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
   Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000002 \ [packed catalog item]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000003[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
```

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000005 \ [packed catalog item]$

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ (0000000000006 [packed catalog item]) \ details \$

Oueries value:

Queries value:

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \noon 00000000017 \[packed catalog item] \queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Queries 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]
 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:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000001 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
- 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000003 \ [displaystring] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ name space_catalog5 \ catalog_entries \ 000000000004 \ [library path]$

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Oueries value:

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Oueries value:

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006[supportednamespace]
 Oueries value:

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

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

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value: HKLM\software\microsoft\windows nt\currentversion[installdate]
Queries value: HKLM\software\microsoft\windows nt\currentversion[digitalproductid]

Queries value:

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup[systemsetupinprogress]

 Queries value:
 HKLM\hardware\description\system[systembiosversion]

 Queries value:
 HKLM\hardware\description\system[videobiosversion]

 Queries value:
 HKLM\system\currentcontrolset\services\disk\enum[0]

Queries value: HKLM\software\d0ddaac5a9[66d841bc]
Queries value: HKLM\software\d0ddaac5a9[3a0ee025]
Queries value: HKCU\software\d0ddaac5a9[3a0ee025]
Queries value: HKCU\software\d0ddaac5a9[66d841bc]
Queries value: HKLM\software\d0ddaac5a9[66d841bc]
Queries value: HKCU\software\d0ddaac5a9[ff93998e]
Queries value: HKCU\software\d0ddaac5a9[ff93998e]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}\category\cite{Acf6-a03a-e3ef65729f3d}\cite{Acf6-a$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [name]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Larrent version \explorer \folder descriptions \folder 3eb 685 db-65f9-4cf6-a03a-e3ef65729f3d \cite{lem:hklmsoftwaremicrosoftwindows} Larrent \cite{lem:hklmsoftwaremicrosoftwindow$

Queries value:

a03a-e3ef65729f3d}[description]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[relative path]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}\ [parsing name]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[infotip]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [localized name]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [icon]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [security]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [stream resource]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresourcetype]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [local redirector \ local \ redirector \ redirector \ local \ redirector \ redirector \ local \ redirector \ redirector \ redirector \ redirector \ redir \ redirector \ redirector \ redirector \ redirector \ redirecto$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[roamable]$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [Stream]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [publish \ expanded path]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ fattributes \ 1$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[foldertypeid]}$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [initfolder \ handler]$

Queries value:

 $\label{lem:hkcu} \mbox{\tt HKCU\software\mbox{\tt microsoft\windows\currentversion\explorer\user\ shell}$

folders[appdata]

Oueries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}(category)$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [name]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parentfolder]$

Queries value:

Oueries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} If the software \mbox{$$ f1b32785-6fba-4fcf-9d55-7b8e7f157091} [relative path]$

Queries value:

 $\label{thm:local-operator} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}parsing name\figure{1}{2}$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091}[infotip]

Queries value:

 $\label{localized} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fill 1532785-6 fba-4fcf-9d55-7b8e7f157091 \cite{10calized} \ [localized name]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}[icon]$

Queries value:

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (f1b32785-6fba-4fcf-1b32785-6fba-4fba-4fcf-1b3278-6fba-4fcf-$

9d55-7b8e7f157091}[streamresource]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[stream resource type]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}[localredirectonly]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [roamable]$

Oueries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{f1b32785-6fba-4fcf-9d55-7b8e7f157091}\[precreate]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [stream]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [publish expanded path]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[attributes]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{5}2785-6fba-4fcf-9d55-7b8e7f157091\fifth{1}{5}foldertypeid\figure{1}{2}$

Queries value:

 $HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} If the lem \label{lem:hklm} If the lem \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} If the lem \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} If the lem \label{lem:hklm} HKLM \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} \label{lem:hklm} Software \label{lem:hklm} \label{lem:hklm} Software \label{lem:hklm} \label{lklm} \la$

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[local appdata]

Oueries value:

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

Queries value:

 $HKLM \ software \ `microsoft \ 'explorer \ 'folder descriptions \ '\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [name]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97} [relative path]$

Queries value:

 $\label{thm:microsoftwindows} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}\[parsing name]\]$

Queries value:

 $\label{lem:hklmsoftware} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \eqref{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97} [infotip]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[localizedname]}$

Queries value:

 $\label{local-ham} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[icon]$

Oueries value:

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

Queries value:

 $\label{lem:hklm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[streamresource]}$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} \ [stream resource type]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} In the constant of the constant of$

Queries value:

 $\label{local-ham} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[precreate]}$

Queries value:

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

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[publishexpandedpath]}$

Queries value:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{62ab5d82-fdc1-4dc3-

a9dd-070d1d495d97}[attributes]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[folder type id]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\}[initfolder handler]$

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]}$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[name]}$

Queries value:

 $HKLM \ software \ `microsoft \ 'current version \ 'explorer \ 'folder descriptions \ '\{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parent folder]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[description]}$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [relative path]$

Queries value:

 $HKLM \ software \ `microsoft \ 'enclosed \ 'enclosed$

Queries value:

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [localized name]$

Queries value:

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [security]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresource]}$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[streamresourcetype]}$

Queries value:

 $\label{thm:microsoft} $HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions \{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localredirectonly]$$

Queries value:

 $\label{thm:local-problem} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [roamable]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[precreate]}$

Queries value:

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}\ [publishexpandedpath]$

Queries value:

 $\label{thm:local-prop} $$HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[attributes]$$

Oueries value:

 $\label{local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [folder type id]$

Queries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[initfolderhandler]}$

Queries value: $HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath]$

Queries value: HKLM\software\microsoft\windows\currentversion\run[]
Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\3[1206]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\3[2300]
Value changes:

HKCU\software\microsoft\windows\currentversion\internet

settings\zones\3[1809]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\1[1206]

Value changes: HKCU\software\microsoft\windows\currentversion\internet

settings\zones\1[2300]

 $\label{thm:condition} Value\ changes: \\ HKCU \ software \ microsoft \ windows \ current version \ internet$

settings\zones\1[1809]