Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 626, Task ID: 2452

Task ID: 2452 Risk Level: 6

Date Processed: 2016-02-22 05:31:58 (UTC)

Processing Time: 29.1 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

6 Tries to detect VM environment

5 Abnormal sleep detected

5 Possible injector

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process:

 $C: \windows \texttt{temp} \texttt{b} 3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe $ ["C: \windows \texttt{temp} \texttt{b} 3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5.exe"]$

Reads from process: PID:432 C:\Windows\explorer.exe

Terminates process:

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \BaseNamedObjects\F00C06EFB1D4349F

Creates mutex: \Sessions\1\BaseNamedObjects\5C5B0BB420F37A88

File System Events

Opens: C:\Windows\Prefetch\B3AF5BCCF7891B0251AAA73F063F1-4CD469AF.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\SysW0W64

C:\Windows\SysWOW64\sechost.dll Opens: Opens: C:\windows\temp\version.dll Opens: C:\Windows\SysWOW64\version.dll Opens: C:\windows\temp\wsock32.dll Opens: C:\Windows\SysWOW64\wsock32.dll Opens: C:\windows\temp\winmm.dll C:\Windows\SysWOW64\winmm.dll Opens: C:\windows\temp\atl.dll Opens: Opens: C:\Windows\SysWOW64\atl.dll Opens: C:\windows\temp\wtsapi32.dll Opens: C:\Windows\SysWOW64\wtsapi32.dll C:\Windows\SysWOW64\imm32.dll Opens:

Opens:

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

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

 $\hbox{C: windows $$\text{temp}$ $$ 34599cdd 80c1 fcc5.EN Opens: } \\$

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

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

Opens: C:\windows\temp\VBoxHook.dll
Opens: C:\Windows\SysWOW64\VBoxHook.dll
Opens: C:\Windows\system\VBoxHook.dll
Opens: C:\Windows\VBoxHook.dll

Opens: C:\Windows\SysWOW64\Wbem\VBoxHook.dll

Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\VBoxHook.dll

Opens: C:\WINDOWS\SysWOW64\drivers\VBoxMouse.sys
Opens: C:\WINDOWS\SysWOW64\drivers\vmmouse.sys
Opens: C:\WINDOWS\SysWOW64\drivers\vmhgfs.sys
Opens: C:\WINDOWS\SysWOW64\drivers\vpc-s3.sys
Opens: C:\WINDOWS\SysWOW64\drivers\vpcubus.sys
Opens: C:\Users\Admin\AppData\Roaming

Opens: C:\Users\Admin\AppData\Local
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll

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

Windows Registry Events

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

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

Creates key: HKCU\software\45d234d165

Creates key: HKLM\software\wow6432node\45d234d165

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

options

Opens key: HKLM\system\currentcontrol\session manager

Opens key: HKLM\software\microsoft\wow64

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

execution options

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

Opens key:

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

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

Opens key: HKLM\system\currentcontrol\set\control\nls\customlocale
Opens key: HKLM\system\currentcontrol\set\control\nls\language
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages
Opens key: HKLM\system\currentcontrol\set\control\mui\uilanguages\en-us

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

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

compatibility

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

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

Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\wow6432node\microsoft\oleaut
Opens key: HKLM\system\currentcontrolset\services\crypt32

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

settings Onens kev

HKLM\software\wow6432node\policies\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

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:

 $\label{local-loc$

Opens key:

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

Opens key:

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

Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens kev:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000000
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:

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\software\wow6432node\microsoft\windows\currentversion\app

paths\wireshark.exe

Opens key: HKLM\software\microsoft\windows\currentversion\app paths\wireshark.exe
Opens key: HKLM\hardware\devicemap\scsi\scsi port 0\scsi bus 0\target id 0\logical

unit id 0

Opens key: HKLM\hardware\description\system

Opens key: HKLM\system\currentcontrolset\services\disk\enum
Opens key: HKLM\software\wow6432node\oracle\virtualbox guest additions

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\wireshark

Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\wireshark

Opens key: HKLM\software\wow6432node\wireshark

Opens key: HKCU\software\wireshark

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

 $\verb|paths\fiddler.exe| \\$

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\wow6432node\microsoft\windows\currentversion\app

paths\fiddler2.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\wow6432node\microsoft\windows\currentversion\uninstall\fiddler2

Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\fiddler2

Opens key: HKLM\software\wow6432node\microsoft\fiddler2

Opens key: HKCU\software\microsoft\fiddler2

Opens key: ${\tt HKCR \backslash software \backslash iein spectors oft \backslash httpanalyzer add on}$

 $Opens \; key: \\ \qquad \qquad \mathsf{HKCU} software \verb|\classes| software \verb|\classes| in spectors of the translation of the$

Opens key: HKCR\iehttpanalyzer.httpanalyzeraddon

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCU} \\ \mathsf{software} \\ \mathsf{classes} \\ \mathsf{iehttpanalyzer.httpanalyzeraddon} \\$

Opens key: HKCR\httpanalyzerstd.httpanalyzerstandalone

Opens key: HKCU\software\classes\httpanalyzerstd.httpanalyzerstandalone

Opens key: HKCR\charles.amf.document

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

HKCR\charles.document Opens key:

Opens key: HKCU\software\classes\charles.document Opens key: HKLM\software\wow6432node\xk72 ltd folder

HKCU\software\xk72 ltd folder Opens key:

Opens key: HKLM\software\wow6432node\vmware, inc.\vmware tools

Opens key: HKLM\software\wow6432node\

HKLM\software\wow6432node\45d234d165\ Opens key:

Opens key: HKCU\software\45d234d165\

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

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

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

Opens key:

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

65f9-4cf6-a03a-e3ef65729f3d}\propertybag

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

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1

Opens key:

 $HKCU \setminus software \setminus microsoft \setminus windows \setminus current \vee explorer \setminus session in follows \cap the following of the fol$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders Opens key:

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$ 6fba-4fcf-9d55-7b8e7f157091}

Opens kev:

6fba-4fcf-9d55-7b8e7f157091}\propertybag

Opens key:

fdc1-4dc3-a9dd-070d1d495d97}

Opens key:

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

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

nt\currentversion\profilelist

Opens key:

0e22-4760-9afe-ea3317b67173}

0e22-4760-9afe-ea3317b67173}\propertybag

HKLM\software\wow6432node\microsoft\windows

nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001

Opens key:

980053277-1733835069-2361817685-1001

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

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Queries value:

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

 $HKLM \setminus system \setminus current control \\ language[installlanguagefallback]$

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

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

us[alternatecodepage]

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

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

Oueries value:

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

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

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] HKLM\software\microsoft\windows Oueries value:

nt\currentversion\gre_initialize[disablemetafiles]

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

nt\currentversion\compatibility32[b3af5bccf7891b0251aaa73f063f1d9e5e72d1433a4f13da34999cdd80c1fcc5]

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

nt\currentversion\windows[loadappinit_dlls]

HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Oueries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings[disableimprovedzonecheck]

Queries value: $\label{lem:hklm} \verb+Kklm\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ settings[security_hklm_only]

Queries value: HKLM\system\currentcontrol\set\control\nls\customlocale[en-us]

Oueries value: HKLM\system\currentcontrol\set\control\nls\extendedlocale[en-us]

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [winsock_registry_version]$

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [namespace_callout]$

Queries value:

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

Queries value:

 $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol_catalog 9 [next_catalog_entry_id]$

Oueries value:

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

Queries 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\000000000002[packedcatalogitem] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000003 \ [packed catalog item] \ Queries \ value:$

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 0000000000004 \ [packed catalog item] \ Queries \ value:$

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem] Queries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 \ catalog_entries \ 0000000000010 \ [packed catalog item] \ Queries \ value:$

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

Queries value.

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

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 000000000001 [library path] \\ Queries \ value:$

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

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

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

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

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[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] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
 Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000003 \ [address family] \ Queries \ value:$

```
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:

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\00000000003[providerinfo] Oueries value:

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

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

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

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

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog \catalog_entries \namespace_entries \na$

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]

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

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

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

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

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

 $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace[library path] \\ Queries \value:$

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]
 Oueries 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]
 Oueries value:

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

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\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\wow6432node\45d234d165[b263933a]Queries value:HKLM\software\wow6432node\45d234d165[44a4d02a]

Queries value: HKCU\software\45d234d165[44a4d02a]
Queries value: HKCU\software\45d234d165[b263933a]

Queries value: HKLM\software\wow6432node\45d234d165[0c1e8766]

Queries value: HKCU\software\45d234d165[0c1e8766]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$

65f9-4cf6-a03a-e3ef65729f3d}[category]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [name]$

Queries value:

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

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [description]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [relative path]$

Oueries value:

 $\label{lem:hklm} HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [infotip]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [localized name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} [icon]$

Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]

Oueries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[streamresource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[stream resource type]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[localredirectonly]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\} \ [roamable]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \mbox{$3eb685db-65f9-4cf6-a03a-e3ef65729f3d} [precreate]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[stream]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[publishexpandedpath]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[attributes]$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[init folder handler]$

Queries value:

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

folders[appdata]

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{fiba} $$Hklm \end{fiba} $$Hklm \end{fiba} $$ \end{fi$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{51532785-66ba-4fcf-9d55-7b8e7f157091}\[name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parent folder]$

Oueries value:

 $HKLM \\ software \\ \\ wow 6432 \\ node \\ \\ microsoft \\ \\ windows \\ \\ current \\ version \\ \\ explorer \\ \\ folder \\ descriptions \\ \\ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \\ [description]$

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[relativepath]}$

Oueries value:

 $\label{local-HKLM} HKLM \ software \ wow 6432 node \ icrosoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [parsing name]$

Queries value:

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{f1b32785-b2785$

6fba-4fcf-9d55-7b8e7f157091}[localizedname]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\}[icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [security]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream resource type]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [local redirectonly]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [precreate]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [stream]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} \ [publish expanded path]$

Oueries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [folder type id]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{f1b32785-6fba-4fcf-9d55-7b8e7f157091\} [initfolder handler]$

Queries value:

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

folders[local appdata]

Queries value:

 $\label{lem:hkkm} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescriptions\currentversion\explorer\folderdescription\explorer\folderdescr$

Queries value:

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

Queries value:

Queries value:

 $\label{thm:local-bound} $HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdots\$

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $\label{thm:local-software-wow6432} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\fo$

Oueries value:

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

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cal{local-bound} $\{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97\} [security] $$$

Queries value:

 $\label{local-software-wow6432-node-microsoft-windows-current-version-explorer-folder-descriptions-folder-description-f$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \calebox{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97} [stream resource type]$

Queries value:

 $\label{local-software-wow6432-node-microsoft-windows-current-version-explorer-folder-descriptions \end{62ab5d82-fdc1-4dc3-a9dd-070d1d495d97} [local-redirectonly]$

Queries value:

 $\label{local-software-wow6432-node-microsoft-windows-current-version-explorer-folder-descriptions-folder-description-f$

Queries value:

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

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Oueries value:

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

Queries value: HKLM\software\microsoft\windows

nt\currentversion\profilelist[programdata]

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[category]}$

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parent folder]$

Queries value:

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

Queries value:

 $\label{local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[relative path]}$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} \ [parsing name]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{5e6c858f-0e22-4760-9afe-ea3317b67173\} [infotip]$

Queries value:

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

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[security]$

Queries value:

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

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} Hklm \end{substitute} explorer \end{substitute} Hklm \end{substitute} explorer \end{substitute} Hklm \end{substitute} explorer \end{substitute} expl$

Queries value:

 $\label{thm:local-continuous} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[localredirectonly]}$

Queries value:

 $\label{lem:hklmsoftwarewow6432node\microsoft\windows\currentversion\explorer\\folderdescriptions\\\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[roamable]$

Queries value:

Oueries value:

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

Queries value:

 $\label{thm:local-bound} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\footnote{1}{5}e6c858f-0e22-4760-9afe-ea3317b67173}\[publishexpanded path]$

Oueries value:

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

Queries value:

 $\label{thm:local-ham} $$HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173\}[foldertypeid]}$

Oueries value:

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001[profileimagepath]

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

settings\zones\3[1206]

 settings\zones\3[1809]
 Value changes:
settings\zones\1[1206]
 Value changes:
settings\zones\1[2300]
 Value changes:

settings\zones\1[1809]

settings\zones\3[2300]
Value changes:

 $\label{thm:linear} $$HKCU\software\microsoft\windows\currentversion\internet $$HKCU\software\microsoft\windows\currentversion\internet $$$In (A) and (A) are $$A$ in the substitution of the substitutio$

 $\label{lem:hkcu} \verb+KKCU\+ software\+ microsoft\+ windows\+ current version\+ internet$

 $\label{thm:local_hammon} \begin{tabular}{ll} HKCU \end{tabular} soft \end{tabular} windows \end{tabular} internet$