Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 251, Task ID: 1005

Task ID: 1005

Risk Level:

Date Processed: 2016-04-28 13:15:09 (UTC)

Processing Time: 61.14 seconds Virtual Environment: IntelliVM

"c:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.exe" **Execution Arguments:**

Sample ID: Type: basic Owner: admin

Label: b9157cdd8f2376b26202cce9b65f1efb

Date Added: 2016-04-28 12:45:16 (UTC)

File Type: PE32:win32:gui File Size: 450907 bytes

b9157cdd8f2376b26202cce9b65f1efb MD5:

SHA256: 38a24c7531054711addae1e035f29a9c5e4772890c023481427945c19e2ef417

Description:

Pattern Matching Results

2 PE: Nonstandard section

4 Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

Anomaly: PE: Contains a virtual section

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

C:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.exe

["C:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex:

Creates event: \KernelObjects\MaximumCommitCondition

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

File System Events

C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches Creates:

Creates: C:\Users\Admin\AppData\Local\Temp\

C:\Users\Admin\AppData\Local\Temp\nsqBE6E.tmp Creates:

Opens: C:\Windows\Prefetch\B9157CDD8F2376B26202CCE9B65F1-19879722.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll Opens: C:\Windows\System32\wow64win.dll C:\Windows\System32\wow64cpu.dll Opens: Opens: C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

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

C:\windows\temp\b9157cdd8f2376b26202cce9b65f1efb.exe.Local\ Opens:

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

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af C:\Windows\winsxs\x86 microsoft.windows.common-Opens:

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

Opens: C:\windows\temp\VERSION.dll C:\Windows\SysWOW64\version.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll C:\Windows\SysWOW64\rpcss.dll Opens: Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\SHFOLDER.DLL Opens: C:\Windows\SysWOW64\shfolder.dll

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

Opens: C:\Windows\SysWOW64\shell32.dll

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

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

C:\Windows\winsxs\x86_microsoft.windows.commoncontrols_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

C:\Windows\WindowsShell.Manifest Opens:

Opens: C:\

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

Opens: $C: \verb|\USers\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db|$

Opens: C:\windows\temp\ntmarta.dll Opens: C:\Windows\SysWOW64\ntmarta.dll

Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-

4C77-AF34-C647E37CA0D9}.1.ver0x00000000000001.db

Opens: C:\Users\Admin\AppData\Local\Temp\nsqBE6E.tmp
Opens: C:\Windows\Temp\b9157cdd8f2376b26202cce9b65f1efb.exe

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

Opens: C:\windows\temp\RichEd20.DLL
Opens: C:\Windows\SysWOW64\riched20.dll
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll

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

Opens: C:\Windows\SysWOW64\ole32.dll

Opens: C:\Windows\win.ini

Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Users\Admin\Desktop\desktop.ini

Reads from: C:\Windows\Temp\b9157cdd8f2376b26202cce9b65f1efb.exe

Reads from: C:\Windows\win.ini

Reads from: C:\Windows\Fonts\StaticCache.dat

Deletes: C:\Users\Admin\AppData\Local\Temp\nsqBE6E.tmp

Windows Registry Events

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

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

execution options

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

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

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

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

Opens key: HKCU\

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

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

Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

Opens key:

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

nt\currentversion\gre_initialize

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

nt\currentversion\compatibility32

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

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:

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

Opens key: ${\tt HKLM \ } {\tt key:} \\ {\tt HKLM \ } {\tt system \ } {\tt current control \ } {\tt lextended locale} \\$

Opens key:

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

Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key:

08002b30309d}\shellfolder

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-

3aea-1069-a2d8-08002b30309d}\shellfolder

Opens key:

a2d8-08002b30309d}\shellfolder

HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key:

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus policies \setminus nonenum \\ in the polici$

Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum

Opens kev:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-

11e3-a68e-806e6f6e6963}\

Opens key: HKCU\software\classes\drive\shellex\folderextensions

Opens key: HKCR\drive\shellex\folderextensions

Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-

4442-804e-409d6c4515e9}

Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-

409d6c4515e9}

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

Opens key: HKLM\software\policies\microsoft\windows\explorer HKCU\software\policies\microsoft\windows\explorer Opens key: HKCU\software\microsoft\windows\currentversion\explorer Opens kev: Opens key: HKCU\software\microsoft\windows\currentversion\explorer\

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

Opens key:

 $HKLM \label{lem:hklm} Which is the last of the last$

Opens key:

HKCU\software\microsoft\windows\shell\associations\urlassociations\directory

Opens key: HKCU\software\classes\directory

Opens key: HKCR\directory

Opens key: HKCU\software\classes\directory\curver

Opens key: HKCR\directory\curver

Opens key: HKCR\directory\

Opens key: HKCU\software\classes\directory\shellex\iconhandler

Opens key: HKCR\directory\shellex\iconhandler Opens key: HKCU\software\classes\folder

Opens key: HKCR\folder

Opens key: HKCU\software\classes\folder\shellex\iconhandler

HKCR\folder\shellex\iconhandler Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

Opens key: HKCU\software\classes\allfilesystemobjects\shellex\iconhandler

Opens key: HKCR\allfilesystemobjects\shellex\iconhandler Opens key: HKCU\software\classes\directory\docobject

Opens key: HKCR\directory\docobject

Opens kev: HKCU\software\classes\folder\docobject

Opens key: HKCR\folder\docobject

Opens key: HKCU\software\classes\allfilesystemobjects\docobject

Opens key: HKCR\allfilesystemobjects\docobject

Opens key: HKCU\software\classes\directory\browseinplace

Opens key: HKCR\directory\browseinplace

Opens key: HKCU\software\classes\folder\browseinplace

HKCR\folder\browseinplace Opens key:

Opens key: HKCU\software\classes\allfilesystemobjects\browseinplace

Opens key: HKCR\allfilesystemobjects\browseinplace Opens key: HKCU\software\classes\directory\clsid

Opens key: HKCR\directory\clsid

Opens key: HKCU\software\classes\folder\clsid

Opens key: HKCR\folder\clsid

Opens key: HKCU\software\classes\allfilesystemobjects\clsid

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-b4bf$

db2c-424c-b029-7fe99a87c641}

Opens key:

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

db2c-424c-b029-7fe99a87c641}\propertybag

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

Opens key:

 $\label{thm:local_hammon_hammon} HKCU \software \microsoft \windows \current version \explorer \session in folders \end{substantable} $$HKCU \software \microsoft \windows \current version \explorer \session \noindent folders \end{substantable} $$HKCU \software \microsoft \windows \current \end{substantable} $$HKCU \software \windows \current \windows \current \end{substantable} $$$HKCU \software \windows \current \windows \current \windows \current \windows \current \windows \current \windows \current \windows \window$

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

folders

Opens key: HKLM\software\microsoft\com3

Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}

Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\treatas Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid Opens kev: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprocserver32 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprocserver32 Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler32 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprochandler32 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprochandler Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\inprochandler Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders Opens key: HKLM\system\currentcontrolset\services\ldap Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: b587-4786-b4ef-bd1dc332aeae} b587-4786-b4ef-bd1dc332aeae}\propertybag Opens key: 65f9-4cf6-a03a-e3ef65729f3d} Opens key: 65f9-4cf6-a03a-e3ef65729f3d}\propertybag Opens key:

0e22-4760-9afe-ea3317b67173}

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{5e6c858f-4c41\} \\ for the first of the first o$ 0e22-4760-9afe-ea3317b67173}\propertybag

Opens key: HKLM\software\wow6432node\microsoft\windows $nt \verb|\currentversion| profile list \verb|\s-1-5-21-980053277-1733835069-2361817685-1001| list list \verb|\s-1-5-21-980053277-1733885-1001| list \verb|\s-1-5-21-98005327-1001| list \verb|\s-1-5-21-9800$

Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-

980053277-1733835069-2361817685-1001

Opens key: HKLM\system\currentcontrolset\control\cmf\config

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

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

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

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

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

Opens key: HKLM\system\setup

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

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

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

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-11e3-a68e-806e6f6e6963}\

Opens key: ${\tt HKLM \ } system \verb|\ current control \ \\ set \verb|\ control \ \\ locale$

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

Opens key:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be07 - be07 - be07 - be08 -$ Opens key:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} $HKLM \setminus software \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be$ Opens kev: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

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

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

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

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback Opens kev: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui HKLM\software\microsoft\windows Opens key: nt\currentversion\languagepack\surrogatefallback\ms shell dlg 2 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter] HKLM\system\currentcontrolset\control\session Queries value: manager[cwdillegalindllsearch] Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty] Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] HKLM\system\currentcontrolset\control\mui\uilanguages\en-Oueries value: us[alternatecodepage] Queries value: HKCU\control panel\desktop[preferreduilanguages] Oueries value: $\label{local-control} \mbox{ HKCU\control panel\desktop\muicached[machinepreferreduilanguages]} \label{local-control}$ Queries value: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ side by side [prefer external manifest]$ Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[b9157cdd8f2376b26202cce9b65f1efb] HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\windows[loadappinit_dlls] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: $\label{prop:linear} HKLM \software \microsoft \windows \current version \policies \explorer \cite{Microsoft} no properties \mbox{\it mycomputer} \end{microsoft}$ Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[attributes] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[callforattributes] Oueries value: 08002b30309d}\shellfolder[restrictedattributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsfordisplay] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[hidefolderverbs] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[usedrophandler] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsforparsing] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsparsedisplayname] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[queryforoverlay] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[mapnetdriveverbs] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforinfotip] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[hideinwebview] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[hideondesktopperuser] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsaliasednotifications] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsuniversaldelegate] $HKCR \verb+wow6432+ node \verb+clsid++ \{20d04fe0-3aea-1069-a2d8-4444\} + \{20d04fe0-3aea-1069-a2d8-444\} + \{20d04fe0-3aea-1060-a2d8-444\} + \{20d04fe0-3aea-1060-a2d8-444$ Oueries value: 08002b30309d}\shellfolder[nofilefolderjunction] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[pintonamespacetree] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[hasnavigationenum]

```
Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
   Queries value:
11e3-a68e-806e6f6e6963}[data]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[generation]
                                                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
   Queries value:
409d6c4515e9}[drivemask]
   Oueries value:
Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
   Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
   Oueries value:
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ [dont pretty path]) \ downward \ (explorer \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ (explorer \ advanced \ advanced \ advanced \ advanced \ advanced \ advanced \ adva
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
   Oueries value:
                                                HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
   Oueries value:
HKCU \ software \ microsoft \ windows \ current version \ explorer \ advanced [nonetcrawling]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
   Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
   Queries value:
                                                HKCR\directory[docobject]
   Queries value:
                                                HKCR\folder[docobject]
   Queries value:
                                                HKCR\allfilesystemobjects[docobject]
   Queries value:
                                                HKCR\directory[browseinplace]
   Oueries value:
                                                HKCR\folder[browseinplace]
   Queries value:
                                                HKCR\allfilesystemobjects[browseinplace]
   Queries value:
                                                HKCR\directory[isshortcut]
   Queries value:
                                                HKCR\folder[isshortcut]
   Queries value:
                                                HKCR\allfilesystemobjects[isshortcut]
   Queries value:
                                                HKCR\directory[alwaysshowext]
                                                HKCR\directory[nevershowext]
   Queries value:
                                                HKCR\folder[nevershowext]
   Oueries value:
   Queries value:
                                                HKCR\allfilesystemobjects[nevershowext]
   Queries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{b4bfcc3a-bc1, b4bfcc3a-bc2, b4
db2c-424c-b029-7fe99a87c641}[category]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[name]
   Oueries value:
db2c-424c-b029-7fe99a87c641}[parentfolder]
db2c-424c-b029-7fe99a87c641}[description]
   Queries value:
db2c-424c-b029-7fe99a87c641}[relativepath]
   Oueries value:
```

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma[]{\colorer.pdf} \end{subarrange} Abstraction \colorer.$

Queries value:

Oueries value

 $\label{localized} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} [icon]$

Oueries value:

 $\label{thm:local-prop} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \begin{center} b4bfcc3a-db2c-424c-b029-7fe99a87c641 \end{center} \]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} [stream resource]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3adb2c-424c-b029-7fe99a87c641\} [stream resource type]$

Oueries value:

 $\label{local-continuous} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\gamma\gamm$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [roamable]$

Queries value

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [publish \ expanded \ path]$

Oueries value:

 $\label{linear_ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folder descriptions\folder descriptions\folder\folde$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\fill\foldertypeid\g$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [initfolder \ handler]$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[desktop]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[inprocserver32]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[]

Queries value: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]

Queries value:

HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]

Queries value:HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]Queries value:HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]Queries value:HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]

Queries value:

 $\label{thm:local-basis} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\category\]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [parent folder]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [description]$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{lem:hklmsoftware}\cite{lem:hklmsoftw$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} \ [parsing name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [infotip]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [localized name]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [icon]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [security]$

Queries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream resource]$

Ougries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [stream resource type]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [local redirectonly]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [roamable]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[precreate]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[stream]$

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae)\cite{lem:hklmsoftware}\cite{lem:hklmsoftw$

Oueries value

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}[attributes]$

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [folder type id]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\} [initfolder \ handler]$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432} HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folds folds folds \folds \folds$

Oueries value:

 $\label{lem:hklmsoftware} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d\}[parsing name]$

Queries value:

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{3eb685db-16422 \\ node \setminus \{3eb68$ 65f9-4cf6-a03a-e3ef65729f3d}[precreate]

Oueries value:

 $HKLM \label{lem:hklm} Which was the statement of the st$ 65f9-4cf6-a03a-e3ef65729f3d}[stream]

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ before \ folder \ folde$ 65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

Oueries value:

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

folders[appdata]

Queries value:

0e22-4760-9afe-ea3317b67173}[category]

Oueries value:

0e22-4760-9afe-ea3317b67173}[name]

Queries value:

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

0e22-4760-9afe-ea3317b67173}[description]

Oueries value:

0e22-4760-9afe-ea3317b67173}[relativepath]

Oueries value:

0e22-4760-9afe-ea3317b67173}[parsingname]

Queries value:

0e22-4760-9afe-ea3317b67173}[infotip]

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

Queries value:

0e22-4760-9afe-ea3317b67173}[icon]

Oueries value:

0e22-4760-9afe-ea3317b67173}[security]

Queries value:

0e22-4760-9afe-ea3317b67173}[streamresource]

Queries value:

0e22-4760-9afe-ea3317b67173}[streamresourcetype]

Oueries value:

0e22-4760-9afe-ea3317b67173}[localredirectonly]

Oueries value:

0e22-4760-9afe-ea3317b67173}[roamable]

Queries value:

0e22-4760-9afe-ea3317b67173}[precreate]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]

Oueries value:

0e22-4760-9afe-ea3317b67173}[publishexpandedpath]

Oueries value:

0e22-4760-9afe-ea3317b67173}[attributes]

Oueries value:

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

```
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
                                       HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
  Oueries value:
980053277-1733835069-2361817685-1001[profileimagepath]
                                       HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:
  Queries value:
                                       HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
                                       HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
                                       HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
  Queries value:
                                       HKLM\software\microsoft\rpc[maxrpcsize]
  Oueries value:
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Oueries value:
                                       HKLM\system\setup[oobeinprogress]
  Queries value:
                                       HKLM\system\setup[systemsetupinprogress]
                                       HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
  Oueries value:
11e3-a68e-806e6f6e6963}[data]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
11e3-a68e-806e6f6e6963}[generation]
                                       HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:
  Queries value:
                                       HKLM\system\currentcontrolset\control\nls\language groups[1]
                                       HKLM \setminus software \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 - b
  Oueries value:
0 fb 58b 01c 4a 4 \} \\ language profile \\ (0x 000 000 000) \\ \{0001 bea 3-ed 56-48 3 d-a 2e 2-a ea e 25 5774 36\} [enable]
                                       HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:
  Oueries value:
                                       HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Queries value:
                                       HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:
                                       HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:
                                       HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Queries value:
                                       HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Queries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Oueries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Oueries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
                                       HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane3]
                                       HKLM\software\microsoft\windows
  Oueries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane4]|
  Queries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
                                       HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane7]
                                       HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                                       HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane9]
                                       HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane10]
                                       HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
  Oueries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
                                       HKLM\software\microsoft\windows
  Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
                                       HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:
                                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
```

HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane16]

Oueries value: