Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 68, Task ID: 273

Task ID: 273

Risk Level: 1

Date Processed: 2016-04-28 12:54:29 (UTC)

Processing Time: 61.1 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe"

Sample ID: 68
Type: basic
Owner: admin

Label: 1edab3297a51c34ae2782d399a89b328

Date Added: 2016-04-28 12:44:56 (UTC)

File Type: PE32:win32:gui File Size: 360448 bytes

MD5: 1edab3297a51c34ae2782d399a89b328

SHA256: 86ab6c7b128b020d5a9a6fc179576b65f1b021b7e915ce512be2fb24393d70dc

Description: None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe

["C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1

Creates event: \KernelObjects\MaximumCommitCondition

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

Creates semaphore: \Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?

1EDAB3297A51C34AE2782D399A89B328.EXE

File System Events

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

Opens: C:\Windows\Prefetch\1EDAB3297A51C34AE2782D399A89B-849703DA.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dl1
Opens: C:\Windows\System32\wow64win.dl1
Opens: C:\Windows\System32\wow64cpu.dl1
Opens: C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64

 Opens:
 C:\windows\temp\MSVBVM60.DLL

 Opens:
 C:\Windows\SysW0W64\msvbvm60.dl1

 Opens:
 C:\Windows\SysW0W64\sechost.dl1

 Opens:
 C:\Windows\SysW0W64\imm32.dl1

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

Opens: C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe.cfg

 Opens:
 C:\windows\temp\SXS.DLL

 Opens:
 C:\Windows\SysWOW64\sxs.dl1

 Opens:
 C:\Windows\System32\C_932.NLS

 Opens:
 C:\Windows\System32\C_949.NLS

 Opens:
 C:\Windows\System32\C_950.NLS

 Opens:
 C:\Windows\System32\C_936.NLS

 Opens:
 C:\Program Files (x86)

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

Opens: C:\windows\temp\1edab3297a51c34ae2782d399a89b328.exe.Local\

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

controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\

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

Opens: C:\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.ver0x000000000000001.db

Opens: C:\Program Files (x86)\desktop.ini
Opens: C:\Windows\SysWOW64\scrrun.dll

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

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

Opens: C:\Windows\Temp

Opens: C:\windows\temp\audomate4.ini Opens: C:\windows\temp\audomate.mdb C:\Windows\Fonts\StaticCache.dat Opens: Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll C:\Windows\SysWOW64\ole32.dll Opens: Reads from: C:\Program Files (x86)\desktop.ini C:\Windows\SysWOW64\scrrun.dll Reads from: Reads from: C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

 $\label{thm:local_hammon} \mbox{HKLM\software\mbox{\sc hilbs.} indows nt\current version\sc file execution} \\$ Opens key:

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\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

HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens kev: 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: $\label{thm:local_machine} \begin{tabular}{ll} HKCU \control panel \desktop \muicached \machine language configuration \end{tabular} \label{thm:local_machine}$ Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

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

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

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

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

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

options\dllnxoptions

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

nt\currentversion\gre_initialize

HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32

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

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\control\nls\extendedlocale

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

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

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

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

Opens key: HKLM\system\currentcontrolset\control\nls\codepage Opens key: HKLM\software\wow6432node\microsoft\vba\monitors

Opens key: HKCU\software\classes\ Opens key: HKLM\software\microsoft\com3

Opens kev: HKCU\software\classes\wow6432node\clsid\{2e2c5836-6406-4e06-99a7-

e8e8cae58e8b}

Opens key: HKCR\wow6432node\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b} Opens key: HKCU\software\classes\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b}

Opens key: HKCR\clsid\{2e2c5836-6406-4e06-99a7-e8e8cae58e8b} Opens key: HKLM\software\wow6432node\diepol\audomate4\

Opens key:

Opens key:

c1bf-494e-b29c-65b732d3d21a}

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus current version \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus \{905e63b6-microsoft \setminus windows \setminus explorer \setminus folder descriptions \setminus explorer \setminus folder \in explorer \setminus explorer \setminus folder \cap explorer \setminus expl$

c1bf-494e-b29c-65b732d3d21a}\propertybag Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-descriptions\} \\ for the first of the$ a0fb-4bfc-874a-c0f2e0b9fa8e} a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag Opens kev: HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer HKLM\software\microsoft\windows\currentversion\policies\explorer Opens key: Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer Opens key: $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 1edab 3297 a 51c 34ae 2782 d 399a 89b 328. exe$ Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots HKCU\software\classes\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens key: 08002b30309d}\shellfolder HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Opens kev: 08002b30309d}\shellfolder $HKCU \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus clsid \setminus \{20d04fe0-delta \} + \{20d04f$ Opens key: 3aea-1069-a2d8-08002b30309d}\shellfolder Opens kev: a2d8-08002b30309d}\shellfolder HKCU\software\microsoft\windows\currentversion\policies\nonenum Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\policies\nonenum Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume Opens kev: 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} HKLM\software\wow6432node\policies\microsoft\windows\explorer Opens key: Opens key: HKLM\software\policies\microsoft\windows\explorer Opens key: HKCU\software\policies\microsoft\windows\explorer Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d} Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\treatas Opens key: $HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as$ Opens key: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\progid Opens key: $HKCR \ wow 6432 node \ clsid \ \{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\} \ \ progid$ Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\progid Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprocserver32 HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens key: b8dc300d9f9d}\inprocserver32 HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-Opens kev: b8dc300d9f9d}\inprochandler32 Opens key: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50b8dc300d9f9d}\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

 00a0c9054228}
 Opens key:
 HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\

 00a0c9054228}\treatas
 HKCD\www(432sada) alaid\{0d43fe01-f093-11cf-8940-00a0c9054228\}

Opens key:

Opens key:

Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas

HKLM\system\currentcontrolset\services\ldap

HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

Opens key: $\label{local-bound} \begin{tabular}{ll} HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228\}\progid} \end{tabular}$

Opens key: $HKCR\wow6432 node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\ \ progid$ Opens kev: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32

Opens key: HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprocserver32

Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprochandler32

HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-Opens key:

00a0c9054228}\inprochandler32

Opens key: HKCU\software\classes\wow6432node\clsid\{0d43fe01-f093-11cf-8940-

00a0c9054228}\inprochandler

HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-Opens key:

00a0c9054228}\inprochandler

HKCU\software\classes\typelib Opens key:

Opens key: HKCR\typelib

Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}

Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0 Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0

Opens key: HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0 Opens key: HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-

00a0c9054228}\1.0\0\win32

HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32 Opens key:

Opens kev: HKLM\svstem\currentcontrolset\control\cmf\config

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

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

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:

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

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

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback

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

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ ctf \ compatibility \ 1edab 3297a 51c 34ae 2782d 399a 89b 328.exe$ Opens key: $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus ctf \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 -$

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} Opens kev: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

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

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

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

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

Queries value:

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

Oueries value:

HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries 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\system\currentcontrolset\control\nls\sorting\versions[] Queries value: ${\tt HKLM \ } system \verb| current control \verb| session manager[safedll sear chmode] \\$ Queries value:

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]

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

options\dllnxoptions[msvbvm60.dll]

Oueries value:

HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[1edab3297a51c34ae2782d399a89b328] Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

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

manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [category]$

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [name]$

Queries value:

 $\label{thm:local-ham} $HKLM \sim \frac{905e63b6-c1bf-494e-b29c-65b732d3d21a}{[parentfolder]} $$$

Queries value:

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

Queries value:

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

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} \ [parsing name]$

Oueries value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cdot \{905e63b6-c1bf-494e-b29c-65b732d3d21a\} [infotip]$

Queries value:

 $\label{thm:localized} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \equal 1000 folder \cite{1000} and \cite{10000} and \cite{1000} and \cite{1000} and \cite{1000} and \cite{1000} and$

Queries value:

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\[security]$

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[streamresource]

Oueries value

 $\label{thm:microsoftwindows} HKLM software \noindows \$

Queries value

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

Oueries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\cdot\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}\cdot{locality} \end{substitute} In the context of the context o$

Queries value:

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

Queries value

 $\label{lem:hklmsoftware} HKLM software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \cite{2000} folder \ci$

Queries value:

 $\label{lem:hklmsoftwarewow6432node} Hklm\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\{905e63b6-c1bf-494e-b29c-65b732d3d21a\}[publishexpandedpath]$

Queries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-c1bf-494e-b29c-65b732d3d21a}[foldertypeid]

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \gamma \finite folder handler\]$

Queries value:

 $HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version [program files dir]$

Oueries value

 $\label{thm:local_explorer} \begin{tabular}{ll} HKLM \end{tabular} $$HKLM \end{tabular} $$ HKLM \end{tabular} $$ exclaim \end{tabular} $$ exclaim$

```
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
     Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
     Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
     Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
     Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
     Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \
a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
     Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
     Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \
a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
     Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
     Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
     Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus current \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus \{7c5a40ef-microsoft \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus windows \setminus windows \setminus windows \\ descriptions \setminus windows \\ descriptions \setminus windows \setminus windows \\ descriptions \setminus windows
a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
     Queries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
     Oueries value:
HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{7c5a40ef-microsoft \ windows \ explorer \ folder \ descriptions \ explorer \ folder \
a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes1
     Oueries value:
a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
     Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
     Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
     Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
     Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
     Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Queries value:
08002b30309d}\shellfolder[attributes]
     Oueries value:
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}\shellfolder[callforattributes]
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}\shellfolder[restrictedattributes]
     Oueries value:
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
 08002b30309d}\shellfolder[wantsfordisplay]
                                                                        HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
     Oueries value:
```

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

08002b30309d}\shellfolder[hidefolderverbs]

Oueries value:

```
08002b30309d}\shellfolder[usedrophandler]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsforparsing]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforoverlay]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[mapnetdriveverbs]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[queryforinfotip]
  Oueries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[hideinwebview]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[hideondesktopperuser]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[wantsaliasednotifications]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[wantsuniversaldelegate]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
  Queries value:
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\shellfolder[pintonamespacetree]
                                   HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[hasnavigationenum]
  Oueries value:
HKLM \ software \ microsoft \ windows \ current version \ policies \ nonenum \ [\{20d04fe0-3aea-1069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8-4069-a2d8
08002b30309d}1
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-
11e3-a68e-806e6f6e6963}[data]
11e3-a68e-806e6f6e6963}[generation]
                                   HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Oueries value:
409d6c4515e9}[drivemask]
  Queries value:
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}[]
  Oueries value:
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
  Oueries value:
b8dc300d9f9d}\inprocserver32[]
  Queries value:
                                   HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}\inprocserver32[threadingmodel]
  Oueries 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:
                                   HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\progid[]
                                   HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]
  Oueries value:
                                   HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
  Queries value:
00a0c9054228}\inprocserver32[inprocserver32]
                                   HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
  Queries value:
00a0c9054228}\inprocserver32[]
                                   HKCR\wow6432node\clsid\{0d43fe01-f093-11cf-8940-
  Oueries value:
00a0c9054228}\inprocserver32[threadingmodel]
                                   HKLM\system\currentcontrolset\control\cmf\config[system]
  Oueries value:
  Queries value:
                                   HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
  Queries value:
                                   HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
Queries value:
                                   HKLM\system\setup[oobeinprogress]
  Oueries value:
                                   HKLM\system\setup[systemsetupinprogress]
  Queries value:
                                   HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
                                   HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]
  Oueries value:
11e3-a68e-806e6f6e6963}[data]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-
11e3-a68e-806e6f6e6963}[generation]
  Oueries value:
                                   HKLM\software\microsoft\windows
\verb|nt\current| version \verb|\language| pack \verb|\datastore\_v1.0[disable]|
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Oueries value:
                                   HKLM\software\microsoft\windows
```

```
nt\currentversion\languagepack\surrogatefallback[plane3]
                         HKI M\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane4]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane6]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\languagepack\surrogatefallback[plane7]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
```