# Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 162, Task ID: 649

Task ID: 649 Risk Level: 4

Date Processed: 2016-04-28 13:04:50 (UTC)

Processing Time: 2.66 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\62f72b9f37a7cd2eae5ecce3744c4df1.exe"

Sample ID: 162 Type: basic Owner: admin

Label: 62f72b9f37a7cd2eae5ecce3744c4df1

Date Added: 2016-04-28 12:45:07 (UTC)

File Type: PE32:win32:gui File Size: 193824 bytes

MD5: 62f72b9f37a7cd2eae5ecce3744c4df1

SHA256: ef75f5b747ed1023051220c89ee6e8f4a6c44315fd67487968a97d688c91e71c

Description: None

### 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

Creates process: C:\windows\temp\62f72b9f37a7cd2eae5ecce3744c4df1.exe

["C:\windows\temp\62f72b9f37a7cd2eae5ecce3744c4df1.exe"]

Terminates process: C:\Windows\Temp\62f72b9f37a7cd2eae5ecce3744c4df1.exe

### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \KernelObjects\MaximumCommitCondition

### File System Events

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

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

Creates: C:\Users\Admin\AppData\Local\Temp\nszE33B.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp

Creates: C:\Users
Creates: C:\Users\Admin

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

Creates: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\System.dll

Creates: C:\Program Files (x86)

Creates: C:\Program Files (x86)\Mozilla Maintenance Service
Creates: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\nsExec.dll

Creates: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe
Opens: C:\Windows\Prefetch\62F72B9F37A7CD2EAE5ECCE3744C4-71B63C57.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\SysWOW64\sechost.dll

Opens: C:\windows\temp\62f72b9f37a7cd2eae5ecce3744c4df1.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\temp\VERSION.dll C:\Windows\SysWOW64\version.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\WindowsShell.Manifest C:\Windows\SysWOW64\rpcss.dll Opens: Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\SHFOLDER.DLL Opens: C:\Windows\SysWOW64\shfolder.dll

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

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

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:\Users\Admin\Desktop\desktop.ini
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll
Opens: C:\Users\Admin\AppData\Local\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\nszE33B.tmp
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

Opens: C:\Windows\Temp\62f72b9f37a7cd2eae5ecce3744c4df1.exe

Opens: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp

Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData

Opens: C:\Users\Admin\AppData\Local

Opens: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\System.dll

Opens: C:\Program Files (x86)

Opens: C:\Program Files (x86)\Mozilla Maintenance Service

Opens: C:\Windows\Temp

Opens: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\nsExec.dll

Opens: C:\Program Files (x86)\Mozilla Maintenance

Service\maintenanceservice.exe

Opens: C:\Program Files (x86)\Mozilla Maintenance

Service\maintenanceservice.exe.exe

Opens: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe
Opens: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe\

Writes to: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\System.dl1
Writes to: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\nsExec.dl1

Writes to: C:\Program Files (x86)\Mozilla Maintenance Service\Uninstall.exe

Reads from: C:\Users\Admin\Desktop\desktop.ini

Reads from: C:\Windows\Temp\62f72b9f37a7cd2eae5ecce3744c4df1.exe
Deletes: C:\Users\Admin\AppData\Local\Temp\nszE33B.tmp
Deletes: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\nsExec.dll
Deletes: C:\Users\Admin\AppData\Local\Temp\nspE34C.tmp\System.dll

## Windows Registry Events

Creates key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ mozillama intenances er vice \ model \ mozillama intenances \ mozillama \$ 

Creates key: HKLM\software\mozilla\maintenanceservice

Creates key: HKLM\software

Creates key: HKLM\software\mozilla

Deletes value: HKLM\software\mozilla\maintenanceservice[ffprefetchdisabled]

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\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\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\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:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key: HKLM\syste

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 62f72b9f37a7cd2eae5ecce3744c4df1.exe$ 

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

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

08002b30309d}\shellfolder

 $Opens~key: \\ \qquad \qquad \text{HKCU} software \verb|\microsoft| windows \verb|\currentversion| explorer \verb|\clsid| {20d04fe0-persion| explorer| clsid| explorer| clsid| {20d04fe0-persion| explorer| clsid| explorer| cl$ 

3aea-1069-a2d8-08002b30309d\shellfolder

Opens key:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ (20d04fe0-3aea-1069-104) \ described \ (20d04fe0-3aea-1069-$ 

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

Opens key:

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}

 $Opens~key: \\ HKCR\drive\shellex\folder extensions\fbeb8a05-beee-4442-804e-folder extensions\folder e$ 

409d6c4515e9}

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

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

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

Opens key:

 $HKLM \label{lem:hklm} Which was shell registered applications \label{lklm} Which was shell registered applications \labe$ 

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

Opens key: HKCR\folder\shellex\iconhandler

Opens key: HKCU\software\classes\allfilesystemobjects

Opens key: HKCR\allfilesystemobjects

 $Opens~key: \\ \qquad \qquad \text{HKCU} software \verb|\classes| all filesystemobjects| shellex \verb|\iconhandler| \\$ 

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

Opens key: HKCR\directory\docobject

Opens key: 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

Opens key: HKCR\folder\browseinplace

 $Opens\ key: \\ HKCU \ software \ classes \ all file system objects \ browsein place$ 

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:

db2c-424c-b029-7fe99a87c641}

Opens key:

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

 $HKCU \ software \ microsoft \ windows \ current version \ explorer \ session in following \ the constant of the constant in the constant of the constant of$ Opens key:

Opens key:

HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders

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-8f50-

 $b8dc300d9f9d} \land treatas$ 

 $HKCR\wow6432 node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treat as$ Opens key: Opens kev: HKCU\software\classes\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\progid

Opens key:  $HKCR\wow6432$ node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key:

HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d} Opens key: Opens key: HKCU\software\classes\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\progid

Opens key: HKCR\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\progid

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprocserver32

Opens key:  $HKCU \setminus software \setminus classes \setminus wow 6432 \\ node \setminus clsid \setminus \{1f486a52 - 3cb1 - 48fd - 8f50 - 48fd - 8f50$ 

b8dc300d9f9d}\inprochandler32

Opens kev: HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key:  $HKLM \setminus system \setminus current control \\ \setminus lsa \setminus access providers$ 

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings

Opens key:

b587-4786-b4ef-bd1dc332aeae}

Opens key:

b587-4786-b4ef-bd1dc332aeae}\propertybag

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{3eb685db-10explorer\} \ folder \ between the constant \ folder \ between the constant \ folder \ fold$ 65f9-4cf6-a03a-e3ef65729f3d}

Opens key:

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

Opens key:

0e22-4760-9afe-ea3317b67173}

Opens key:

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

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

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

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:

 $HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d3-8213-64}$ 

11e3-a68e-806e6f6e6963}\

Opens key: HKLM\software\wow6432node\mozilla\maintenanceservice

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

options\dllnxoptions

Opens key: HKLM\software\mozilla\maintenanceservice

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

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

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

options[disableusermodecallbackfilter]

Queries value:  ${\tt HKLM \ } system \verb|\ current control \ session$ 

manager[cwdillegalindllsearch]

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]

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]

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

Oueries value:

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

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]

HKLM\software\wow6432node\microsoft\windows Queries value: nt\currentversion\compatibility32[62f72b9f37a7cd2eae5ecce3744c4df1] Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value:

 $HKLM \label{lem:hklm} \verb| hklm \| software \| microsoft \| windows \| current version \| policies \| explorer \| no properties my computer \| explorer \| expl$ 

Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]

HKLM\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]

Queries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value:

HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]

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

08002b30309d}\shellfolder[attributes]

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

08002b30309d}\shellfolder[callforattributes]

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

08002b30309d}\shellfolder[restrictedattributes]

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

08002b30309d}\shellfolder[wantsfordisplay]

 $HKCR \verb|\wow6432| node \verb|\clsid| \{20d04fe0-3aea-1069-a2d8-4aea-1060-a2d8-4aea-10$ Oueries value: 08002b30309d}\shellfolder[hidefolderverbs]

Oueries value:

HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[usedrophandler]

Oueries value:

08002b30309d}\shellfolder[wantsforparsing] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-

08002b30309d}\shellfolder[wantsparsedisplayname]

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

08002b30309d}\shellfolder[queryforoverlay]

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

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]

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

08002b30309d}\shellfolder[hideondesktopperuser]

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

08002b30309d}\shellfolder[wantsaliasednotifications]

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

08002b30309d}\shellfolder[wantsuniversaldelegate]

```
HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-4444}
  Oueries value:
08002b30309d}\shellfolder[nofilefolderjunction]
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
  Queries value:
08002b30309d}\shellfolder[pintonamespacetree]
  Queries value:
                                     HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
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 \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus mountpoints 2 \setminus cpc \setminus volume \setminus \{8063a3d4-8213-mountpoints 2 \setminus cpc \setminus volume \setminus \{8063a3d4-8213-mountpoints 2 \setminus cpc \setminus volume \}
11e3-a68e-806e6f6e6963}[data]
11e3-a68e-806e6f6e6963}[generation]
                                     HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
  Oueries value:
409d6c4515e9}[drivemask]
  Queries value:
HKLM \verb|\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]|
                                     HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Oueries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
  Oueries value:
                                     \label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced \cite{tabular} hidden \cite{tabular} \end{tabular}
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
                                     HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Queries value:
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
  Oueries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
                                     HKCR\directory[docobject]
  Oueries value:
  Queries value:
                                     HKCR\folder[docobject]
  Queries value:
                                     HKCR\allfilesystemobjects[docobject]
  Queries value:
                                     HKCR\directory[browseinplace]
                                     HKCR\folder[browseinplace]
  Queries value:
                                     HKCR\allfilesystemobjects[browseinplace]
  Oueries value:
  Queries value:
                                     HKCR\directory[isshortcut]
  Queries value:
                                      HKCR\folder[isshortcut]
  Queries value:
                                     HKCR\allfilesystemobjects[isshortcut]
  Oueries value:
                                      HKCR\directory[alwaysshowext]
  Oueries value:
                                     HKCR\directorv[nevershowext]
  Queries value:
                                     HKCR\folder[nevershowext]
  Queries value:
                                     HKCR\allfilesystemobjects[nevershowext]
  Oueries value:
db2c-424c-b029-7fe99a87c641}[category]
db2c-424c-b029-7fe99a87c641}[name]
  Queries value:
db2c-424c-b029-7fe99a87c641}[parentfolder]
```

Oueries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

 $HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\gamma\folderdescriptions\gamma\folderdescriptions\gamma\gamma\gamma\folderdescriptions\gamma\gam$ 

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

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:

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:

 $\label{local-ham} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\f(1b3ea5dc-b587-4786-b4ef-bd1dc332aeae\}\category\cite{Ab3}$ 

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value

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

Ougries value

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

Queries value:

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

Oueries 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:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Oueries 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:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value

Queries value:

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

Oueries value:

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

Queries value:

 $HKLM\software\wow6432$ node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]

Queries value:

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

Queries value:

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

Queries value:

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

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}[localredirectonly]

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

folders[appdata]

Queries value:

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

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

Oueries value:

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

Queries value:

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

Queries value:

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

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-

0e22-4760-9afe-ea3317b67173}[roamable] Oueries value:

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

Oueries value:

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

Oueries value:

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

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

Queries value:

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

Queries value:

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

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

980053277-1733835069-2361817685-1001[profileimagepath]

Queries value: HKLM\system\currentcontrol\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error

reporting\wmr[disable]

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:

HKLM\system\currentcontrol\set\control\computername[computername]

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

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

Queries value:

11e3-a68e-806e6f6e6963}[data]

Queries value:

11e3-a68e-806e6f6e6963}[generation]

Oueries value:

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

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[system.dll]

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

options\dllnxoptions[nsexec.dll]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]

Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayname]
 Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[uninstallstring]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayicon]
Sets/Creates value:

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[displayversion]
 Sets/Creates value:

 $\label{lem:hklmsoftware} HKLM \software \wow 6432 node \microsoft \windows \current version \uninstall \mozilla maintenance service [publisher] \software \wow 6432 node \microsoft \windows \current version \uninstall \mozilla maintenance \software \mozilla maintenance \software \mozilla maintenance \software \mozilla maintenance \software \mozilla \m$ 

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ mozillama intenances er vice [comments] Sets/Creates value:$ 

HKLM\software\wow6432node\microsoft\windows\currentversion\uninstall\mozillamaintenanceservice[nomodify] Sets/Creates value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ uninstall \ mozillama intenances ervice [estimated size] \ mozillama \ moz$ 

Sets/Creates value: HKLM\software\mozilla\maintenanceservice[attempted]
Sets/Creates value: HKLM\software\mozilla\maintenanceservice[installed]