Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 131, Task ID: 525

Task ID: 525

Risk Level: 4

Date Processed: 2016-04-28 13:01:23 (UTC)

Processing Time: 3.22 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a3d6128a1b210860531603f74a24c7f.exe"

Sample ID: 131
Type: basic
Owner: admin

Label: 2a3d6128a1b210860531603f74a24c7f

Date Added: 2016-04-28 12:45:03 (UTC)

File Type: PE32:win32:gui File Size: 620911 bytes

MD5: 2a3d6128a1b210860531603f74a24c7f

SHA256: cca1510e63a3ab7c4679ab5043dd4c3e0ba1dfcabc2e36c67edd3d46793a8134

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\2a3d6128a1b210860531603f74a24c7f.exe

["C:\windows\temp\2a3d6128a1b210860531603f74a24c7f.exe"]

Terminates process: C:\Windows\Temp\2a3d6128a1b210860531603f74a24c7f.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\nsbC11.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsbC12.tmp
Creates: C:\Users\Admin\AppData\Local\Temp\nsqC22.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\nsqC22.tmp\nsHelper.dll
Opens: C:\Windows\Prefetch\2A3D6128A1B210860531603F74A24-4C63C17E.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\2a3d6128a1b210860531603f74a24c7f.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: C:\Windows\SysWOW64\imm32.dll Opens: Opens: C:\Windows\WindowsShell.Manifest Opens: C:\Windows\SysWOW64\rpcss.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\SHFOLDER.DLL ${\tt C:\Windows\SysWOW64\shfolder.dll}$ Opens:

 ${\tt Opens:} \qquad {\tt C:\Windows\Globalization\Sorting\SortDefault.nls}$

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

Opens: C:\

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

C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\cversions.1.db Opens:

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

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

C:\Users\Admin\AppData\Local\Temp\nsbC11.tmp Opens: C:\Windows\Temp\2a3d6128a1b210860531603f74a24c7f.exe Opens:

C:\Windows\SysWOW64\en-US\setupapi.dll.mui Opens: Opens: C:\Users\Admin\AppData\Local\Temp\nsqC22.tmp

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

C:\Users\Admin\AppData\Local\Temp\nsqC22.tmp\nsHelper.dll Opens:

C:\Program Files (x86)\XingHaoLyrics\ Opens: Opens: C:\Program Files (x86)\LyricsPal\

Writes to: C:\Users\Admin\AppData\Local\Temp\nsbC12.tmp

C:\Users\Admin\AppData\Local\Temp\nsqC22.tmp\nsHelper.dll Writes to:

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

C:\Windows\Temp\2a3d6128a1b210860531603f74a24c7f.exe Reads from: Reads from: C:\Users\Admin\AppData\Local\Temp\nsbC12.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsbC11.tmp Deletes: C:\Users\Admin\AppData\Local\Temp\nsqC22.tmp

Deletes: C:\Users\Admin\AppData\Local\Temp\nsqC22.tmp\nsHelper.dll

Windows Registry Events

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

options

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\wow64

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

execution options

Opens key: HKLM\system\currentcontrolset\control\safeboot\option Opens key:

Opens key:

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

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

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots

 $\label{thm:local_ham} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \control \end{tabular} versions$ Opens key:

Opens key: HKLM\ Opens key:

HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics

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

nt\currentversion\gre_initialize

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

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

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:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ shell compatibility \ applications \ 2a3d 6128a1b210860531603f74a24c7f. exemple \ applications \ and \ applications \ applica$

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

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

Opens key:

a2d8-08002b30309d}\shellfolder

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

Opens key:

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

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

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \end{tabular} \label{thm:linear}$

Opens key:

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
Opens key: HKCU\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\advanced

Opens key:

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: ${\tt HKCU \setminus software \setminus classes \setminus all filesystem objects}$

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 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\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: ${\tt HKCU \setminus software \setminus classes \setminus allfilesystemobjects \setminus clsid}$

Opens key: HKCR\allfilesystemobjects\clsid

Opens key:

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

 $HKLM \software \wow6432 node \microsoft \windows \current version \explorer \folder descriptions \folder \fo$

db2c-424c-b029-7fe99a87c641}

Opens key:

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

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

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}

b8dc300d9f9d}\treatas

Opens key: $\label{local-claid-limit} \begin{tabular}{ll} HKCR\wow6432node\clsid\f1f486a52-3cb1-48fd-8f50-b8dc300d9f9d\treatas \\ Opens key: \\ HKCU\software\classes\wow6432node\clsid\f1f486a52-3cb1-48fd-8f50-\\ \end{tabular}$

b8dc300d9f9d}\progid

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

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

b8dc300d9f9d}\inprocserver32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler32

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

b8dc300d9f9d}\inprochandler

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

b8dc300d9f9d}\inprochandler

Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders

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

Opens key:

Opens key:

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

Opens key:

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

Opens key:

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

Opens key:

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

Opens key

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} e6c858f-0e22-4760-9afe-ea3317b67173\}$

Opens key:

 $\label{thm:local-objective} HKLM\software\wow6432 node\microsoft\windows\currentversion\explorer\folderdescriptions\footnote{1}{0}e22-4760-9afe-ea3317b67173\propertybag$

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

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

Opens key: $\label{lem:hklm} \mbox{HKLM} software \mbox{\sc microsoft} \mbox{\sc mt} \mbox{\sc mt}$

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

 $Opens\ key: \\ HKLM\software\wow6432 node\microsoft\windows\windows\ error\ reporting\wmrex \\ windows\ erro$

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

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:

 $HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d3-8213-11e3-a68e-806e6f6e6963\} \label{eq:hkcu}$

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

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

settings Opens key:

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

settings

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

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

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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] HKLM\system\currentcontrolset\control\nls\customlocale[empty] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback] Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type] Oueries value: HKLM\system\currentcontrolset\control\mui\uilanguages\enus[alternatecodepage] HKCU\control panel\desktop[preferreduilanguages] Oueries value: Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages] Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[] Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value: Queries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\gre_initialize[disablemetafiles]|\\$ HKLM\software\wow6432node\microsoft\windows Oueries value: nt\currentversion\compatibility32[2a3d6128a1b210860531603f74a24c7f] Oueries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls] HKLM\software\microsoft\ole[pageallocatorusesystemheap] Oueries value: Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer] Oueries 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] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nointerneticon] HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: Queries 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] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[callforattributes] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[restrictedattributes] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[wantsfordisplay] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[hidefolderverbs] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[usedrophandler] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsforparsing] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: 08002b30309d}\shellfolder[wantsparsedisplayname] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[queryforoverlay] Oueries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[mapnetdriveverbs] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 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-Queries value: 08002b30309d}\shellfolder[wantsaliasednotifications] Queries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsuniversaldelegate] Oueries value: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[nofilefolderjunction] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Oueries value: 08002b30309d}\shellfolder[pintonamespacetree] HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-Queries value: $08002b30309d \} \verb|\shellfolder[hasnavigationenum]|$

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[data]

Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{8063a3d4-8213-11e3-a68e-806e6f6e6963}[data]

08002b30309d}]
Oueries value:

 $HKCU \software \microsoft \windows \current version \explorer \mountpoints 2 \cpc \volume \ \{8063a3d4-8213-11e3-a68e-806e6f6e6963\} \cline{200} \clin$

Oueries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}[drivemask] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate] Oueries value: $HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus policies \setminus explorer [nowebview]$ HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell] Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling] Oueries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu] HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden] Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor] Oueries value: Oueries value: Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip] Oueries value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \current version \explorer \advanced [hideicons] \end{tabular}$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview] Oueries value: $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \windows \current version \explorer \advanced [filter] \end{tabular}$ HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden] Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling] Oueries 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] Oueries value: HKCR\directory[docobject] HKCR\folder[docobject] Oueries value: Queries value: HKCR\allfilesystemobjects[docobject] HKCR\directory[browseinplace] Queries value: Queries value: HKCR\folder[browseinplace] Queries value: HKCR\allfilesystemobjects[browseinplace] HKCR\directory[isshortcut] Oueries value: HKCR\folder[isshortcut] Queries value: Oueries value: HKCR\allfilesvstemobjects[isshortcut] Queries value: HKCR\directory[alwaysshowext] Queries value: HKCR\directory[nevershowext] Queries value: HKCR\folder[nevershowext] Queries value: HKCR\allfilesystemobjects[nevershowext] Oueries value: db2c-424c-b029-7fe99a87c641}[category] Oueries value: db2c-424c-b029-7fe99a87c641}[name] db2c-424c-b029-7fe99a87c641}[parentfolder] Queries value: db2c-424c-b029-7fe99a87c641}[description] Oueries value: db2c-424c-b029-7fe99a87c641}[relativepath] Oueries value: db2c-424c-b029-7fe99a87c641}[parsingname] db2c-424c-b029-7fe99a87c641}[infotip] Queries value:

db2c-424c-b029-7fe99a87c641}[localizedname]

Oueries value:

db2c-424c-b029-7fe99a87c641}[icon]

Queries value:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus windows \setminus current \\ version \setminus explorer \setminus folder \\ descriptions \setminus \{b4bfcc3a-based \\ in the folder \\ description \\ on the folder \\ on the fold$ db2c-424c-b029-7fe99a87c641}[security]

 $db2c-424c-b029-7fe99a87c641\} [streamresource] \\$

Oueries value:

db2c-424c-b029-7fe99a87c641}[streamresourcetype]

Oueries value:

 $HKLM \label{lem:hklm} Which is the latest and the$ db2c-424c-b029-7fe99a87c641}[localredirectonly]

db2c-424c-b029-7fe99a87c641}[roamable]

Oueries value:

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

Oueries value:

db2c-424c-b029-7fe99a87c641}[stream]

Queries value:

db2c-424c-b029-7fe99a87c641}[publishexpandedpath]

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3adb2c-424c-b029-7fe99a87c641}[attributes]

Queries value:

db2c-424c-b029-7fe99a87c641}[foldertypeid]

Oueries value:

db2c-424c-b029-7fe99a87c641}[initfolderhandler]

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

folders[desktop]

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

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

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

b8dc300d9f9d}\inprocserver32[inprocserver32]

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

b8dc300d9f9d}\inprocserver32[]

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

b8dc300d9f9d}\inprocserver32[threadingmodel]

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

Queries value:

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

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity] $HKLM \verb|\system| current controlset \verb|\services|| ldap[use old host resolution order]$ Oueries value: HKLM\system\currentcontrolset\services\ldap[usehostnameasalias] Queries value: Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[category]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[name]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parentfolder]

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

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[relativepath]

Oueries value:

b587-4786-b4ef-bd1dc332aeae}[parsingname]

Queries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \ \{1b3ea5dc-b2442 node \ microsoft \ windows \ \ \ \ \}$ b587-4786-b4ef-bd1dc332aeae}[infotip]

Oueries value:

 $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ explorer \ folder descriptions \ \{1b3ea5dc-b264, 1b3ea5dc-b264, 1$ b587-4786-b4ef-bd1dc332aeae}[localizedname]

Oueries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dcb587-4786-b4ef-bd1dc332aeae}[icon]

Oueries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries 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:

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

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:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Oueries value:

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

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:

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

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}[roamable]

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Oueries value:

Oueries value:

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

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

folders[appdata]

Queries value:

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

Oueries value:

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

Queries value

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

Queries value:

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

Oueries value:

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

Queries value:

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

Queries value:

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

Oueries value:

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

Oueries value:

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

Queries value:

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

Oueries value

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

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

Queries value:

$$\label{local-prop} \begin{split} HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\folderdescription$$

Queries value:

 $\label{thm:local-bound} HKLM \software \wow 6432 node \microsoft \windows \current version \explorer \folder descriptions \footnote{1.5} Ge6c858f-0e22-4760-9 af e-ea3317b67173 \cite{1.5} [publish expanded path]$

Queries value:

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

Oueries value:

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

Queries value:

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

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:

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]

Oueries value:

11e3-a68e-806e6f6e6963}[generation]

Queries value:

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

HKLM\system\currentcontrolset\services\crypt32[debugheapflags] Queries value: Queries value: $HKLM \verb|\software\\| wow 6432 node\\| microsoft\\| windows\\| current version\\| internet$

settings[disableimprovedzonecheck]

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

settings[security_hklm_only]

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