Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	45
Risk Level:	5
Date Processed:	2016-04-28 12:47:02 (UTC)
Processing Time:	4.77 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\a54d769e8d6fc84c80d6799bfd403ee4.exe"

Sample ID:	12
Type:	basic
Owner:	admin
Label:	a54d769e8d6fc84c80d6799bfd403ee4
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	37888 bytes
MD5:	a54d769e8d6fc84c80d6799bfd403ee4
SHA256:	151c701a631e8ed0107fc96fb7ebd7ba3461acd835db3cd4ead41a154a545349
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
5	Packer: UPX
5	PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\windows\temp\a54d769e8d6fc84c80d6799bfd403ee4.exe ["C:\windows\temp\a54d769e8d6fc84c80d6799bfd403ee4.exe"]
Terminates process:	C:\Windows\Temp\a54d769e8d6fc84c80d6799bfd403ee4.exe

Named Object Events

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

File System Events

Opens:	C:\Windows\Prefetch\A54D769E8D6FC84C80D6799BFD403-A0D094D7.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\a54d769e8d6fc84c80d6799bfd403ee4.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\propsys.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\wow64

```
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\system\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\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                HKLM\
  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\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:                HKCU\software\borland\locales
  Opens key:                HKCU\software\borland\delphi\locales
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\webroot\window washer\paths
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\a54d769e8d6fc84c80d6799bfd403ee4.exe
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\explorer
  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:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{031e4825-
7b94-4dc3-b131-e946b44c8dd5}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{04731b67-
d933-450a-90e6-4acd2e9408fe}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-
e366-4d22-bc06-4ada335c892b}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{26ee0668-
a00a-44d7-9371-beb064c98683}
```

```
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{4336a54d-
038b-4685-ab02-99bb52d3fb8b}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-
ad25-11d0-98a8-0800361b1103}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{5399e694-
6ce5-4d6c-8fce-1d8870fdcba0}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-
5081-101b-9f08-00aa002f954e}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{64693913-
1c21-4f30-a98f-4e52906d3b56}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{89d83576-
6bd1-4c86-9454-beb04e94c819}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{9343812e-
1c37-4a49-a12e-4b2d810d956b}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{98f275b4-
4fff-11e0-89e2-7b86dfd72085}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{a00ee528-
ebd9-48b8-944a-8942113d46ac}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{b4fb3f98-
c1ea-428d-a78a-d1f5659cba93}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{bd7a2e7b-
21cb-41b2-a086-b309680c6b7e}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{daf95313-
e44d-46af-be1b-cbacea2c3065}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{e345f35f-
9397-435c-8f95-4e922c26259e}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{ed228fdf-
9ea8-4870-83b1-96b02cfe0d52}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{edc978d6-
4d53-4b2f-a265-5805674be568}
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{f02c1a0d-
be21-4350-88b0-7367fc96ef3c}
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\delegatefolders
   Opens key:                  HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\delegatefolders
   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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-3aea-1069-
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:                  HKCU\software\classes\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder
   Opens key:                  HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder
   Opens key:                  HKCU\software\microsoft\windows\currentversion\explorer\clsid\{208d2c60-
3aea-1069-a2d7-08002b30309d}\shellfolder
   Opens key:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{208d2c60-3aea-1069-
a2d7-08002b30309d}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{645ff040-
5081-101b-9f08-00aa002f954e}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{645ff040-5081-101b-
9f08-00aa002f954e}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-
a00a-44d7-9371-beb064c98683}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{26ee0668-a00a-44d7-
9371-beb064c98683}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{59031a47-3f72-44a7-
89c5-5595fe6b30ee}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{031e4825-
7b94-4dc3-b131-e946b44c8dd5}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{031e4825-7b94-4dc3-
b131-e946b44c8dd5}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{04731b67-
d933-450a-90e6-4acd2e9408fe}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{04731b67-d933-450a-
90e6-4acd2e9408fe}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{11016101-
e366-4d22-bc06-4ada335c892b}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{11016101-e366-4d22-
bc06-4ada335c892b}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{4336a54d-
038b-4685-ab02-99bb52d3fb8b}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{4336a54d-038b-4685-
ab02-99bb52d3fb8b}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder
   Opens key:                    HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder
   Opens key:                    HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\shellfolder
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{450d8fba-ad25-11d0-
98a8-0800361b1103}\shellfolder
   Opens key:                    HKCU\software\classes\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
```

```
1d8870fdcba0}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{5399e694-
6ce5-4d6c-8fce-1d8870fdcba0}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{5399e694-6ce5-4d6c-
8fce-1d8870fdcba0}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{64693913-
1c21-4f30-a98f-4e52906d3b56}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{64693913-1c21-4f30-
a98f-4e52906d3b56}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{89d83576-
6bd1-4c86-9454-beb04e94c819}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{89d83576-6bd1-4c86-
9454-beb04e94c819}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9343812e-
1c37-4a49-a12e-4b2d810d956b}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{9343812e-1c37-4a49-
a12e-4b2d810d956b}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{98f275b4-
4fff-11e0-89e2-7b86dfd72085}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{98f275b4-4fff-11e0-
89e2-7b86dfd72085}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{a00ee528-
ebd9-48b8-944a-8942113d46ac}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{a00ee528-ebd9-48b8-
944a-8942113d46ac}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{b4fb3f98-
c1ea-428d-a78a-d1f5659cba93}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{b4fb3f98-c1ea-428d-
a78a-d1f5659cba93}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{bd7a2e7b-
21cb-41b2-a086-b309680c6b7e}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{bd7a2e7b-21cb-41b2-
a086-b309680c6b7e}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{daf95313-
e44d-46af-be1b-cbacea2c3065}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{daf95313-e44d-46af-
be1b-cbacea2c3065}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{e345f35f-9397-435c-8f95-
```

```
4e922c26259e}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{e345f35f-
9397-435c-8f95-4e922c26259e}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{e345f35f-9397-435c-
8f95-4e922c26259e}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{ed228fdf-
9ea8-4870-83b1-96b02cfe0d52}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{ed228fdf-9ea8-4870-
83b1-96b02cfe0d52}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{edc978d6-
4d53-4b2f-a265-5805674be568}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{edc978d6-4d53-4b2f-
a265-5805674be568}\shellfolder
  Opens key:                HKCU\software\classes\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder
  Opens key:                HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-
be21-4350-88b0-7367fc96ef3c}\shellfolder
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\clsid\{f02c1a0d-be21-4350-
88b0-7367fc96ef3c}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\app paths\wwdisp.exe
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\wwdisp.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\app paths\wwdisp.exe
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\url\prefixes
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries 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]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:            HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  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]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  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[a54d769e8d6fc84c80d6799bfd403ee4.exe]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[a54d769e8d6fc84c80d6799bfd403ee4]
  Queries value:            HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  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\session manager[safedllsearchmode]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
```

```
 Queries value:              HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer[maximizeapps]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[enableshellexecutehooks]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nopropertiesrecyclebin]
 Queries value:
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]
 Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{031e4825-
7b94-4dc3-b131-e946b44c8dd5}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{04731b67-
d933-450a-90e6-4acd2e9408fe}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-
e366-4d22-bc06-4ada335c892b}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{26ee0668-
a00a-44d7-9371-beb064c98683}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{4336a54d-
038b-4685-ab02-99bb52d3fb8b}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-
ad25-11d0-98a8-0800361b1103}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{5399e694-
6ce5-4d6c-8fce-1d8870fdcba0}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{59031a47-
3f72-44a7-89c5-5595fe6b30ee}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-
5081-101b-9f08-00aa002f954e}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{64693913-
1c21-4f30-a98f-4e52906d3b56}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{89d83576-
6bd1-4c86-9454-beb04e94c819}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{9343812e-
1c37-4a49-a12e-4b2d810d956b}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{98f275b4-
4fff-11e0-89e2-7b86dfd72085}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{a00ee528-
ebd9-48b8-944a-8942113d46ac}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{b4fb3f98-
c1ea-428d-a78a-d1f5659cba93}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{bd7a2e7b-
21cb-41b2-a086-b309680c6b7e}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{daf95313-
e44d-46af-be1b-cbacea2c3065}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{e345f35f-
9397-435c-8f95-4e922c26259e}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{ed228fdf-
9ea8-4870-83b1-96b02cfe0d52}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{edc978d6-
4d53-4b2f-a265-5805674be568}[suppressionpolicy]
 Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\desktop\namespace\{f02c1a0d-
be21-4350-88b0-7367fc96ef3c}[suppressionpolicy]
 Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
```

```
08002b30309d}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
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[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{20d04fe0-3aea-1069-a2d8-
08002b30309d}]
   Queries value:                HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{208d2c60-3aea-1069-a2d7-
08002b30309d}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{208d2c60-3aea-1069-a2d7-
08002b30309d}]
   Queries value:                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{871c5380-42a0-1069-a2ea-
08002b30309d}\shellfolder[foldervalueflags]
   Queries value:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{871c5380-
42a0-1069-a2ea-08002b30309d}\shellfolder[attributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{871c5380-42a0-1069-a2ea-
08002b30309d}]
   Queries value:                HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{645ff040-5081-101b-9f08-
00aa002f954e}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{645ff040-5081-101b-9f08-
00aa002f954e}]
   Queries value:                HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{26ee0668-a00a-44d7-9371-
beb064c98683}]
   Queries value:                HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{59031a47-3f72-44a7-89c5-
5595fe6b30ee}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{59031a47-3f72-44a7-89c5-
5595fe6b30ee}]
   Queries value:                HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{031e4825-7b94-4dc3-b131-
e946b44c8dd5}]
   Queries value:                HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
```

```
4acd2e9408fe}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{04731b67-d933-450a-90e6-
4acd2e9408fe}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{04731b67-d933-450a-90e6-
4acd2e9408fe}]
   Queries value:                  HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{11016101-e366-4d22-bc06-
4ada335c892b}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{11016101-e366-4d22-bc06-
4ada335c892b}]
   Queries value:                  HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{4336a54d-038b-4685-ab02-
99bb52d3fb8b}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{4336a54d-038b-4685-ab02-
99bb52d3fb8b}]
   Queries value:                  HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{450d8fba-ad25-11d0-98a8-
0800361b1103}]
   Queries value:                  HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{5399e694-6ce5-4d6c-8fce-
1d8870fdcba0}]
   Queries value:                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{64693913-1c21-4f30-a98f-
4e52906d3b56}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{64693913-1c21-4f30-a98f-
4e52906d3b56}]
   Queries value:                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{89d83576-6bd1-4c86-9454-
beb04e94c819}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{89d83576-6bd1-4c86-9454-
beb04e94c819}]
   Queries value:                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[attributes]
   Queries value:                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[callforattributes]
   Queries value:                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
4b2d810d956b}\shellfolder[restrictedattributes]
   Queries value:                  HKCR\wow6432node\clsid\{9343812e-1c37-4a49-a12e-
```

```
4b2d810d956b}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9343812e-1c37-4a49-a12e-
4b2d810d956b}]
   Queries value:                HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{98f275b4-4fff-11e0-89e2-
7b86dfd72085}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{98f275b4-4fff-11e0-89e2-
7b86dfd72085}]
   Queries value:                HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{a00ee528-ebd9-48b8-944a-
8942113d46ac}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{a00ee528-ebd9-48b8-944a-
8942113d46ac}]
   Queries value:                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{b4fb3f98-c1ea-428d-a78a-
d1f5659cba93}]
   Queries value:                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{bd7a2e7b-21cb-41b2-a086-
b309680c6b7e}]
   Queries value:                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{daf95313-e44d-46af-be1b-
cbacea2c3065}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{daf95313-e44d-46af-be1b-
cbacea2c3065}]
   Queries value:                HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{e345f35f-9397-435c-8f95-
4e922c26259e}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{e345f35f-9397-435c-8f95-
4e922c26259e}]
   Queries value:                HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[attributes]
   Queries value:                HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[callforattributes]
   Queries value:                HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[restrictedattributes]
   Queries value:                HKCR\wow6432node\clsid\{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}\shellfolder[foldervalueflags]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{ed228fdf-9ea8-4870-83b1-
96b02cfe0d52}]
```

```
  Queries value:             HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder[attributes]
  Queries value:             HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder[callforattributes]
  Queries value:             HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder[restrictedattributes]
  Queries value:             HKCR\wow6432node\clsid\{edc978d6-4d53-4b2f-a265-
5805674be568}\shellfolder[foldervalueflags]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{edc978d6-4d53-4b2f-a265-
5805674be568}]
  Queries value:             HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[attributes]
  Queries value:             HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[callforattributes]
  Queries value:             HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[restrictedattributes]
  Queries value:             HKCR\wow6432node\clsid\{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}\shellfolder[foldervalueflags]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{f02c1a0d-be21-4350-88b0-
7367fc96ef3c}]
```