Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	811
Risk Level:	10
Date Processed:	2016-05-18 10:40:51 (UTC)
Processing Time:	11.61 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"
Sample ID:	3326
Type:	basic
Owner:	admin
Label:	6f21fb21650da014d87426fa0bd8e7f2
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	177664 bytes
MD5:	6f21fb21650da014d87426fa0bd8e7f2
SHA256:	34f1a3cc2318939b243bfc434f9ecfa721574ded9a3958a970d0b817d536885f
Description:	None

Pattern Matching Results

4 Terminates process under Windows subfolder
10 Creates malicious events: Beebone [Trojan]
6 Checks task list from command line

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe ["C:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"]
Creates process:	C:\Windows\SysWOW64\cmd.exe ["C:\Windows\System32\cmd.exe" /c tasklist&&del 6f21fb21650da014d87426fa0bd8e7f2.exe]
Creates process:	\SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
Creates process:	C:\Windows\SysWOW64\tasklist.exe [tasklist]
Terminates process:	C:\Windows\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe
Terminates process:	C:\Windows\SysWOW64\tasklist.exe
Terminates process:	C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP? 6F21FB21650DA014D87426FA0BD8E7F2.EXE

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens:	C:\Windows\Prefetch\6F21FB21650DA014D87426FA0BD8E-9A6B5DAF.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\6f21fb21650da014d87426fa0bd8e7f2.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\winmm.dll
Opens:	C:\Windows\SysWOW64\msvbvm60.dll
Opens:	C:\Windows\SysWOW64\winmmbase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\imm32.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\ole32.dll
Opens:                C:\Windows\SysWOW64\oleaut32.dll
Opens:                C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:                C:\Windows\SysWOW64\uxtheme.dll
Opens:                C:\Windows\SysWOW64\sxs.dll
Opens:                C:\Windows\SysWOW64\clbcatq.dll
Opens:                C:\Windows\Fonts\sserife.fon
Opens:                C:\Windows\SysWOW64\dwmapi.dll
Opens:                C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens:                C:\
Opens:                C:\Windows\SysWOW64\iertutil.dll
Opens:                C:\Windows\SysWOW64\wininet.dll
Opens:                C:\Windows\SysWOW64\secur32.dll
Opens:                C:\Windows\SysWOW64\shlwapi.dll
Opens:                C:\Windows\SysWOW64\shell32.dll
Opens:                C:\Windows\SysWOW64\SHCore.dll
Opens:                C:\Windows\SysWOW64\profapi.dll
Opens:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\counters.dat
Opens:                C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:                C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens:                C:\Windows\WindowsShell.Manifest
Opens:                C:\Windows\SysWOW64\nsi.dll
Opens:                C:\Windows\SysWOW64\ws2_32.dll
Opens:                C:\Windows\SysWOW64\winhttp.dll
Opens:                C:\Windows\SysWOW64\mswsock.dll
Opens:                C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:                C:\Windows\SysWOW64\winnsi.dll
Opens:                C:\Windows\SysWOW64\dnsapi.dll
Opens:                C:\Windows\SysWOW64\cryptsp.dll
Opens:                C:\Windows\SysWOW64\rsaenh.dll
Opens:                C:\Windows\SysWOW64\urlmon.dll
Opens:                C:\Windows\SysWOW64\rasadhlp.dll
Opens:                C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens:                C:\Windows\SysWOW64\dhcpcsvc.dll
Opens:                C:\Windows\System32\Drivers\etc\hosts
Opens:                C:\Windows\SysWOW64\propsys.dll
Opens:                C:\Windows\SysWOW64\cfgmgr32.dll
Opens:                C:\Windows\SysWOW64\devobj.dll
Opens:                C:\Windows\SysWOW64\setupapi.dll
Opens:                C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens:                C:\Users\Admin\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-
4C77-AF34-C647E37CA0D9}.1.ver0x000000000000000e.db
Opens:                C:\Windows\SysWOW64\desktop.ini
Opens:                C:\Windows\SysWOW64\en-US\propsys.dll.mui
Opens:                C:\Users\Admin\Desktop\desktop.ini
Opens:                C:\Windows\SysWOW64\cmd.exe
Opens:                C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Opens:                C:
Opens:                C:\Windows\Globalization
Opens:                C:\Windows\Globalization\Sorting
Opens:                C:\Windows\System32
Opens:                C:\Windows\SysWOW64\wbem
Opens:                C:\Windows\System32\ntdll.dll
Opens:                C:\Windows\System32\wow64win.dll
Opens:                C:\Windows\System32\wow64cpu.dll
Opens:                C:\Windows\System32\kernel32.dll
Opens:                C:\Windows\System32\user32.dll
Opens:                C:\Windows\System32\locale.nls
Opens:                C:\Windows\SysWOW64\wbem\WMIC.exe
Opens:                C:\Windows\WINHELP.INI
Opens:                C:\Windows\System32\conhost.exe
Opens:                C:\Windows\System32\combase.dll
Opens:                C:\Windows\System32\en-US\conhost.exe.mui
Opens:                C:\Windows\System32\ole32.dll
Opens:                C:\Windows\System32\uxtheme.dll
Opens:                C:\Windows\System32\cmd.exe
Opens:                C:\Windows\System32\en-US\cmd.exe.mui
Opens:                C:\Windows\System32\dwmapi.dll
Opens:                C:\Windows\System32\en-US\user32.dll.mui
Opens:                C:\Windows\system32\uxtheme.dll.Config
Opens:                C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
Opens:                C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
Opens:                C:\Windows\System32\SHCore.dll
Opens:                C:\Windows\SysWOW64\tasklist.exe
```

Opens:	C:\Windows\Prefetch\TASKLIST.EXE-178413B7.pf
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\Windows\SysWOW64\framedynos.dll
Opens:	C:\Windows\SysWOW64\netapi32.dll
Opens:	C:\Windows\SysWOW64\dbghelp.dll
Opens:	C:\Windows\SysWOW64\netutils.dll
Opens:	C:\Windows\SysWOW64\srvcli.dll
Opens:	C:\Windows\SysWOW64\wkscli.dll
Opens:	C:\Windows\SysWOW64\en-US\tasklist.exe.mui
Opens:	C:\Windows\SysWOW64\en-US\KernelBase.dll.mui
Opens:	C:\Windows\SysWOW64\wbem\wbemprox.dll
Opens:	C:\Windows\SysWOW64\wbemcomn.dll
Opens:	C:\Windows\SysWOW64\winsta.dll
Opens:	C:\Windows\SysWOW64\wbem\wbemsvc.dll
Opens:	C:\Windows\SysWOW64\wbem\fastprox.dll
Opens:	C:\Windows\SysWOW64\wbem\wmiutils.dll
Opens:	C:\Windows\SysWOW64\wbem\en-US\wmiutils.dll.mui
Opens:	C:\Windows\SysWOW64\en-US\cmd.exe.mui
Reads from:	C:\Windows\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe
Reads from:	C:\Windows\System32\Drivers\etc\hosts
Reads from:	C:\Users\Admin\Desktop\desktop.ini
Reads from:	C:\Windows\SysWOW64\cmd.exe
Reads from:	C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Reads from:	C:\Windows\SysWOW64\tasklist.exe

Network Events

DNS query:	80170.z0dns.com
Sends data to:	0.0.0.0:53
Receives data from:	0.0.0.0:53

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap\
Creates key:	HKLM\software\wow6432node\microsoft\wbem\cimom
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[autodetect]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Deletes value:	HKLM\software\wow6432node\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
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:	HKLM\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\system\currentcontrolset\control\session manager
  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
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  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\
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  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\software\wow6432node\microsoft\ole
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\wow6432node\microsoft\oleaut
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                HKLM\software\wow6432node\microsoft\vba\monitors
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{85847f48-d652-4fd3-9cd1-
3ddafdba1a15}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{85847f48-d652-4fd3-9cd1-
3ddafdba1a15}
  Opens key:                HKCR\wow6432node\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}
  Opens key:                HKCU\software\classes\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}
  Opens key:                HKCR\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}
  Opens key:                HKCU\software\classes\activatableclasses\clsid
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{85847f48-d652-4fd3-9cd1-
3ddafdba1a15}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{a450fe5b-6ab7-4a3c-9cf3-
3cee05d360c1}
  Opens key:                HKCR\activatableclasses\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{a450fe5b-6ab7-4a3c-9cf3-
3cee05d360c1}
  Opens key:                HKCR\wow6432node\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}
  Opens key:                HKCU\software\classes\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}
  Opens key:                HKCR\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{a450fe5b-6ab7-4a3c-9cf3-
3cee05d360c1}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{56d37229-f433-4eef-a6a7-
b69dd0e003a3}
  Opens key:                HKCR\activatableclasses\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{56d37229-f433-4eef-a6a7-
b69dd0e003a3}
  Opens key:                HKCR\wow6432node\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}
  Opens key:                HKCU\software\classes\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}
  Opens key:                HKCR\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{56d37229-f433-4eef-a6a7-
b69dd0e003a3}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{074c6e97-3f4e-4659-9428-
62a3d81a47c1}
  Opens key:                HKCR\activatableclasses\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{074c6e97-3f4e-4659-9428-
62a3d81a47c1}
  Opens key:                HKCR\wow6432node\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}
  Opens key:                HKCU\software\classes\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}
  Opens key:                HKCR\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{074c6e97-3f4e-4659-9428-
62a3d81a47c1}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{98e514e2-7646-40b7-9b56-
9292aacf45cb}
```

```
Opens key:                HKCR\activatableclasses\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb}
Opens key:                HKCU\software\classes\wow6432node\clsid\{98e514e2-7646-40b7-9b56-
9292aacf45cb}
Opens key:                HKCR\wow6432node\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb}
Opens key:                HKCU\software\classes\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb}
Opens key:                HKCR\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb}
Opens key:                HKCU\software\classes\activatableclasses\clsid\{98e514e2-7646-40b7-9b56-
9292aacf45cb}
Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{1ec267b1-9ab3-4fd2-840e-
ec868c13387b}
Opens key:                HKCR\activatableclasses\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b}
Opens key:                HKCU\software\classes\wow6432node\clsid\{1ec267b1-9ab3-4fd2-840e-
ec868c13387b}
Opens key:                HKCR\wow6432node\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b}
Opens key:                HKCU\software\classes\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b}
Opens key:                HKCR\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b}
Opens key:                HKCU\software\classes\activatableclasses\clsid\{1ec267b1-9ab3-4fd2-840e-
ec868c13387b}
Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{f3aaac74-c3f9-4f8e-a603-
5e1ca200bf54}
Opens key:                HKCR\activatableclasses\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54}
Opens key:                HKCU\software\classes\wow6432node\clsid\{f3aaac74-c3f9-4f8e-a603-
5e1ca200bf54}
Opens key:                HKCR\wow6432node\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54}
Opens key:                HKCU\software\classes\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54}
Opens key:                HKCR\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54}
Opens key:                HKCU\software\classes\activatableclasses\clsid\{f3aaac74-c3f9-4f8e-a603-
5e1ca200bf54}
Opens key:                HKLM\system\currentcontrolset\control\cmf\config
Opens key:                HKLM\system\currentcontrolset\services\disk\enum
Opens key:                HKLM\software\wow6432node\microsoft\rpc
Opens key:                HKLM\software\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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}\propertybag
Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key:                HKU\
Opens key:                HKU\.default
Opens key:                HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:                HKCU\software\policies\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\policies\microsoft\internet
explorer\main\featurecontrol
Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
Opens key:                HKCU\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bypass_cache_for_credpolicy_kb936611
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_mappings_for_credpolicy
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_preserve_spaces_in_filenames_kb952730
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\wow6432node\policies
  Opens key:                HKCU\software\policies
  Opens key:                HKCU\software
  Opens key:                HKLM\software\wow6432node
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet explorer
  Opens key:                HKLM\software\policies\microsoft\internet explorer
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:
```

```
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_sch_send_aux_record_kb_2618444
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3b74704e
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:                HKLM\software\policies\microsoft\peerdist\service
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\peerdist\service
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:                HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\system\currentcontrolset\services\dns
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
```

```
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}\propertybag
Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-1923240461-1905901954-2556564120-1001
Opens key:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}\propertybag
Opens key:              HKLM\software\wow6432node\microsoft\rpc\extensions
Opens key:              HKLM\software\microsoft\rpc\extensions
Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{00000323-0000-0000-c000-
000000000046}
Opens key:              HKCR\activatableclasses\clsid\{00000323-0000-0000-c000-000000000046}
Opens key:              HKCU\software\classes\wow6432node\clsid\{00000323-0000-0000-c000-
000000000046}
Opens key:              HKCR\wow6432node\clsid\{00000323-0000-0000-c000-000000000046}
Opens key:              HKCU\software\classes\clsid\{00000323-0000-0000-c000-000000000046}
Opens key:              HKCR\clsid\{00000323-0000-0000-c000-000000000046}
Opens key:              HKCU\software\classes\activatableclasses\clsid\{00000323-0000-0000-c000-
000000000046}
Opens key:              HKCU\software\classes\appid\6f21fb21650da014d87426fa0bd8e7f2.exe
Opens key:              HKCR\appid\6f21fb21650da014d87426fa0bd8e7f2.exe
Opens key:              HKLM\software\wow6432node\microsoft\ole\appcompat
Opens key:              HKLM\software\microsoft\ole\appcompat
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
Opens key:              HKLM\software\policies\microsoft\cryptography
Opens key:              HKLM\software\microsoft\cryptography
Opens key:              HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key:              HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
Opens key:              HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
Opens key:              HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
Opens key:              HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
Opens key:              HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}
Opens key:              HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-4f27df8760d0}
Opens key:              HKCU\software\classes\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32
Opens key:              HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32
Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}
```

```
Opens key:                 HKCR\activatableclasses\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key:                 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}
Opens key:                 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}
Opens key:                 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\treatas
Opens key:                 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}\treatas
Opens key:                 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32
Opens key:                 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32
Opens key:                 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprochandler32
Opens key:                 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprochandler32
Opens key:                 HKCU\software\classes\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprochandler
Opens key:                 HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprochandler
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\
Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains
Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:                 HKLM\zonemap\ranges\
Opens key:                 HKCU\zonemap\ranges\
Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key:                 HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap
Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zonemap\
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:                 HKLM\software\policies\microsoft\internet explorer\security
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\
Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones
Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\0
Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\1
Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
```

Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet

settings\winhttp
  Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters
  Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key: HKLM\software\policies\microsoft\system\dnsclient
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
  Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-25b8d56dd1d8}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-8a6dc56e0da9}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-55779daa70e9}
  Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\applications\6f21fb21650da014d87426fa0bd8e7f2.exe
  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:
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\desktop\namespace
 Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\delegatefolders
 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\cmd.exe
    Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\app
paths\cmd.exe
    Opens key: HKLM\software\microsoft\windows\currentversion\app paths\cmd.exe
    Opens key: HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
    Opens key:

```
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
     Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}\
     Opens key:              HKCU\software\classes\drive\shellex\folderextensions
     Opens key:              HKCR\drive\shellex\folderextensions
     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\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}
     Opens key:              HKLM\system\currentcontrolset\control\deviceclasses\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}\properties
     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:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}\
     Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\
     Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\advanced
     Opens key:              HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32
     Opens key:              HKCU\software\classes\directory
     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:              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:              HKCU\software\classes\allfilesystemobjects\clsid
     Opens key:              HKCR\allfilesystemobjects\clsid
     Opens key:              HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32
     Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{1f486a52-3cb1-48fd-8f50-
b8dc300d9f9d}
     Opens key:              HKCR\activatableclasses\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}
     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}\treatas
     Opens key:              HKCR\wow6432node\clsid\{1f486a52-3cb1-48fd-8f50-b8dc300d9f9d}\treatas
     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\software\wow6432node\microsoft\windows\currentversion\explorer\kindmap
     Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\kindmap
     Opens key:              HKCU\software\classes\.exe
     Opens key:              HKCR\.exe
     Opens key:              HKCU\software\classes\.exe\openwithprogids
```

```
Opens key:          HKCR\.exe\openwithprogids
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe\openwithprogids
Opens key:          HKCU\software\classes\exefile
Opens key:          HKCR\exefile
Opens key:          HKCU\software\classes\exefile\curver
Opens key:          HKCR\exefile\curver
Opens key:          HKCR\exefile\
Opens key:          HKCU\software\classes\exefile\shellex\iconhandler
Opens key:          HKCR\exefile\shellex\iconhandler
Opens key:          HKCU\software\classes\systemfileassociations\.exe
Opens key:          HKCR\systemfileassociations\.exe
Opens key:          HKCU\software\classes\systemfileassociations\.exe\shellex\iconhandler
Opens key:          HKCR\systemfileassociations\.exe\shellex\iconhandler
Opens key:          HKCU\software\classes\exefile\docobject
Opens key:          HKCR\exefile\docobject
Opens key:          HKCU\software\classes\systemfileassociations\.exe\docobject
Opens key:          HKCR\systemfileassociations\.exe\docobject
Opens key:          HKCU\software\classes\exefile\browseinplace
Opens key:          HKCR\exefile\browseinplace
Opens key:          HKCU\software\classes\systemfileassociations\.exe\browseinplace
Opens key:          HKCR\systemfileassociations\.exe\browseinplace
Opens key:          HKCU\software\classes\exefile\clsid
Opens key:          HKCR\exefile\clsid
Opens key:          HKCU\software\classes\systemfileassociations\.exe\clsid
Opens key:          HKCR\systemfileassociations\.exe\clsid
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}\propertybag
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}\propertybag
Opens key:          HKCU\software\classes\exefile\shell
Opens key:          HKCR\exefile\shell
Opens key:          HKCU\software\classes\exefile\shell\open
Opens key:          HKCR\exefile\shell\open
Opens key:          HKCR\wow6432node\clsid\{1649d1cf-deaf-4a68-abe8-
5c9f68572fd1}\inprocserver32
Opens key:          HKCR\exefile\shell\open\
Opens key:          HKCU\software\classes\exefile\shell\open\command
Opens key:          HKCR\exefile\shell\open\command
Opens key:          HKCU\software\classes\exefile\shell\open\droptarget
Opens key:          HKCR\exefile\shell\open\droptarget
Opens key:          HKLM\software\microsoft\windowsruntime\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}
Opens key:          HKCR\activatableclasses\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
Opens key:          HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}
Opens key:          HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
Opens key:          HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\treatas
Opens key:          HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas
Opens key:          HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32
Opens key:          HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32
Opens key:          HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler32
Opens key:          HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler32
Opens key:          HKCU\software\classes\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler
Opens key:          HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler
Opens key:          HKLM\software\microsoft\windowsruntime\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
Opens key:          HKCR\activatableclasses\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key:          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}
Opens key:          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
Opens key:          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
Opens key:          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
Opens key:          HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
Opens key:          HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
```

```
Opens key:              HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
Opens key:              HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
Opens key:              HKCU\software\classes\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
Opens key:              HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
Opens key:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
Opens key:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
Opens key:              HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
Opens key:              HKLM\software\microsoft\telemetryclient\throttlestore\sqm
Opens key:              HKLM\software\microsoft\telemetryclient\throttlestore
Opens key:              HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
Opens key:              HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
Opens key:              HKLM\software\microsoft\telemetryclient\samplestore\sqm
Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
Opens key:              HKCU\software\classes\exefile\progid
Opens key:              HKCR\exefile\progid
Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\shellcompatibility\progids\exefile
Opens key:              HKCU\software\classes\exefile\shell\open\ddeexec
Opens key:              HKCR\exefile\shell\open\ddeexec
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
Opens key:              HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key:              HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key:              HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key:              HKLM\software\policies\microsoft\windows\appcompat
Opens key:              HKCU\software\microsoft\windows nt\currentversion
Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key:              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
Opens key:              HKCU\software\classes\applications\cmd.exe
Opens key:              HKCR\applications\cmd.exe
Opens key:              HKCU\software\microsoft\windows\shell\associations
Opens key:              HKLM\software\wow6432node\microsoft\windows
Opens key:              HKLM\software\wow6432node\microsoft\windows\html help
Opens key:              HKLM\software\wow6432node\microsoft\windows\help
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\conhost.exe
Opens key:              HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:              HKLM\system\currentcontrolset\control\error message instrument\
Opens key:              HKLM\system\currentcontrolset\control\error message instrument
Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:              HKLM\software\microsoft\oleaut
Opens key:              HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
Opens key:              HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
Opens key:              HKCU\console
Opens key:              HKCU\console\
Opens key:              HKCU\console\%systemroot%_system32_cmd.exe
Opens key:              HKCU\console\%systemroot%\system32\cmd.exe
```

```
Opens key:              HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
Opens key:              HKLM\software\microsoft\ctf\compatibility\conhost.exe
Opens key:              HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:              HKCU\software\policies\microsoft\windows\system
Opens key:              HKLM\software\wow6432node\microsoft\command processor
Opens key:              HKCU\software\microsoft\command processor
Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tasklist.exe
Opens key:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\tasklist.exe
Opens key:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\tasklist.exe
Opens key:              HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key:              HKLM\software\wow6432node\microsoft\wbem\cimom
Opens key:              HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
Opens key:              HKCU\software\classes\appid\tasklist.exe
Opens key:              HKCR\appid\tasklist.exe
Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}
Opens key:              HKCR\activatableclasses\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key:              HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}
Opens key:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key:              HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\treatas
Opens key:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
Opens key:              HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
Opens key:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
Opens key:              HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
Opens key:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
Opens key:              HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
Opens key:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}
Opens key:              HKCR\activatableclasses\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key:              HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}
Opens key:              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key:              HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\treatas
Opens key:              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
Opens key:              HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
Opens key:              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
Opens key:              HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
Opens key:              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
Opens key:              HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler
Opens key:              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler
Opens key:              HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}
Opens key:              HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
Opens key:              HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
Opens key:              HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}
Opens key:              HKCR\activatableclasses\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key:              HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}
Opens key:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key:              HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\treatas
Opens key:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
Opens key:              HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
Opens key:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
Opens key:              HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
```

```
00aa004b2e24}\inprochandler32
   Opens key:                HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler
   Opens key:                HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler
   Opens key:                HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}
   Opens key:                HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
   Opens key:                HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
   Opens key:                HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
   Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}
   Opens key:                HKCR\activatableclasses\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
   Opens key:                HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}
   Opens key:                HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
   Opens key:                HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\treatas
   Opens key:                HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
   Opens key:                HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32
   Opens key:                HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler32
   Opens key:                HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler
   Opens key:                HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler
   Opens key:                HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}
   Opens key:                HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
   Opens key:                HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
   Opens key:                HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
   Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}
   Opens key:                HKCR\activatableclasses\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
   Opens key:                HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}
   Opens key:                HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
   Opens key:                HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\treatas
   Opens key:                HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
   Opens key:                HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
   Opens key:                HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler32
   Opens key:                HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler
   Opens key:                HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler
   Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}
   Opens key:                HKCR\activatableclasses\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
   Opens key:                HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}
   Opens key:                HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}
   Opens key:                HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\treatas
   Opens key:                HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}\treatas
   Opens key:                HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32
   Opens key:                HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler32
   Opens key:                HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler32
   Opens key:                HKCU\software\classes\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprochandler
   Opens key:                HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
```

```
252725d697ca}\inprochandler
  Opens key:              HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}
  Opens key:              HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}
  Opens key:              HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32
  Opens key:              HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32
  Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}
  Opens key:              HKCR\activatableclasses\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}
  Opens key:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\treatas
  Opens key:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32
  Opens key:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler32
  Opens key:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler
  Opens key:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler
  Opens key:              HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}
  Opens key:              HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
  Opens key:              HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32
  Opens key:              HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32
  Opens key:              HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}
  Opens key:              HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
  Opens key:              HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32
  Opens key:              HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32
  Opens key:              HKLM\software\microsoft\windowsruntime\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}
  Opens key:              HKCR\activatableclasses\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}
  Opens key:              HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}
  Opens key:              HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\treatas
  Opens key:              HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}\treatas
  Opens key:              HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprocserver32
  Opens key:              HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprocserver32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprochandler32
  Opens key:              HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprochandler32
  Opens key:              HKCU\software\classes\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprochandler
  Opens key:              HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprochandler
  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\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\dllnxoptions[usefilter]
    Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[msvbvm60.dll]
    Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[6f21fb21650da014d87426fa0bd8e7f2]
    Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
    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\system\currentcontrolset\control\nls\customlocale[en-us]
    Queries value:             HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
    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:             HKLM\system\currentcontrolset\control\nls\locale[00000409]
    Queries value:             HKLM\system\currentcontrolset\control\nls\language groups[1]
    Queries value:             HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
    Queries value:             HKLM\software\microsoft\sqmclient\windows[ceipenable]
    Queries value:             HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
    Queries value:             HKLM\system\currentcontrolset\control\nls\codepage[932]
    Queries value:             HKLM\system\currentcontrolset\control\nls\codepage[949]
    Queries value:             HKLM\system\currentcontrolset\control\nls\codepage[950]
    Queries value:             HKLM\system\currentcontrolset\control\nls\codepage[936]
    Queries value:             HKLM\software\microsoft\com3[com+enabled]
    Queries value:             HKLM\software\microsoft\ole[maxsxshashcount]
    Queries value:             HKLM\system\currentcontrolset\control\cmf\config[system]
    Queries value:             HKLM\system\currentcontrolset\services\disk\enum[0]
    Queries value:             HKLM\software\microsoft\rpc[maxrpcsize]
    Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
    Queries value:             HKLM\system\setup[oobeinprogress]
    Queries value:             HKLM\system\setup[systemsetupinprogress]
    Queries value:             HKLM\software\microsoft\rpc[idletimerwindow]
    Queries value:             HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
    Queries value:             HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
    Queries value:
```

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
    Queries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[cache]
    Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
    Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
    Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
    Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
    Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
    Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[preconnectlimit]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[preresolvelimit]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sqmhttpstreamrandomuploadpoolsize]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
    Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
    Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
    Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
    Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings[enablenegotiate]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]

    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[bypassslnocachecheck]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypassslnocachecheck]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
    Queries value:

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
```

```
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
    Queries value:          HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
    Queries value:          HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[usefirstavailable]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[combinefalsestartdata]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[disablefalsestartblacklist]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[enforcep3pvalidity]
    Queries value:          HKLM\software\microsoft\windows
nt\currentversion\peerdist\service[enable]
    Queries value:          HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Queries value:          HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
    Queries value:          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[autodetect]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
    Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
    Queries value:          HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
```

```
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
    Queries value:                HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
    Queries value:                HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartnameresolution]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
    Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
    Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
    Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
    Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[newdhcpsrvregistration]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresource]
```

```
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[initfolderhandler]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[precreate]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[attributes]
```

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}[initfolderhandler]
    Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001[profileimagepath]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-

65f9-4cf6-a03a-e3ef65729f3d}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[security]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[relativepath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[parsingname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[infotip]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[localizedname]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[icon]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[security]

```
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[streamresource]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[streamresourcetype]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[initfolderhandler]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
    Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
    Queries value:              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
    Queries value:              HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
    Queries value:              HKLM\software\microsoft\ole[defaultaccesspermission]
    Queries value:              HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
    Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
    Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
    Queries value:              HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
    Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
    Queries value:              HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
    Queries value:              HKLM\software\microsoft\cryptography[machineguid]
    Queries value:              HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
    Queries value:              HKCR\wow6432node\interface\{a168aadc-1674-49da-ad4f-
4f27df8760d0}\proxystubclsid32[]
    Queries value:              HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-60ce2149e33c}[]
    Queries value:              HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[inprocserver32]
    Queries value:              HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[]
    Queries value:              HKCR\wow6432node\clsid\{057eee47-2572-4aa1-88d7-
60ce2149e33c}\inprocserver32[threadingmodel]
    Queries value:              HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
    Queries value:              HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingcheck]
    Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
    Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
    Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
    Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
    Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
    Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
    Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
    Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
```

settings[createuricachesize]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
  Queries value:
HKLM\system\currentcontrolset\services\winhttpautoproxysvc\parameters[proxydllfile]
  Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[winhttplowercasehost]
  Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
  Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-

806e6f6e6963}[dhcpnameserver]
    Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[enablemulticast]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[queryadaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disableadapterdomainname]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disabledynamicupdate]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enableadapterdomainnameregistration]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationmaxaddresscount]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[maxnumberofaddressestoregister]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enablemulticast]
    Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
    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}]
    Queries value:              HKCR\wow6432node\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32[]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
    Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
    Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
    Queries value:              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[data]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nowebview]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c63-7c88-
11e3-be65-806e6f6e6963}[generation]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[classicshell]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
    Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
```

Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[autocheckselect]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[iconsonly]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showtypeoverlay]
    Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
    Queries value: HKCR\wow6432node\clsid\{a07034fd-6caa-4954-ac3f-
97a27216f98a}\inprocserver32[]
    Queries value: HKCR\directory[docobject]
    Queries value: HKCR\folder[docobject]
    Queries value: HKCR\allfilesystemobjects[docobject]
    Queries value: HKCR\directory[browseinplace]
    Queries value: HKCR\folder[browseinplace]
    Queries value: HKCR\allfilesystemobjects[browseinplace]
    Queries value: HKCR\directory[isshortcut]
    Queries value: HKCR\folder[isshortcut]
    Queries value: HKCR\allfilesystemobjects[isshortcut]
    Queries value: HKCR\directory[alwaysshowext]
    Queries value: HKCR\directory[nevershowext]
    Queries value: HKCR\folder[nevershowext]
    Queries value: HKCR\allfilesystemobjects[nevershowext]
    Queries value: HKCR\wow6432node\clsid\{75847177-f077-4171-bd2c-
a6bb2164fbd0}\inprocserver32[]
    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\windows\currentversion\policies\explorer[allowfileclsidjunctions]
    Queries value: HKLM\software\microsoft\windows\currentversion\explorer\kindmap[.exe]
    Queries value: HKCR\.exe[content type]
    Queries value: HKCR\.exe[]
    Queries value: HKCR\exefile[docobject]
    Queries value: HKCR\systemfileassociations\.exe[docobject]
    Queries value: HKCR\exefile[browseinplace]
    Queries value: HKCR\systemfileassociations\.exe[browseinplace]
    Queries value: HKCR\exefile[isshortcut]
    Queries value: HKCR\systemfileassociations\.exe[isshortcut]
    Queries value: HKCR\exefile[alwaysshowext]
    Queries value: HKCR\systemfileassociations\.exe[alwaysshowext]
    Queries value: HKCR\exefile[nevershowext]
    Queries value: HKCR\systemfileassociations\.exe[nevershowext]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[category]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[name]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[parentfolder]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[description]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-
db2c-424c-b029-7fe99a87c641}[relativepath]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[icon]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[streamresourcetype]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[localredirectonly]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[roamable]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[precreate]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[stream]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[publishexpandedpath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[attributes]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[foldertypeid]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[desktop]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[category]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[name]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parentfolder]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[description]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[relativepath]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[parsingname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[infotip]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[localizedname]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[icon]
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[security]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresource]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}[streamresourcetype]

Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[localredirectonly]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[roamable]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[precreate]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[stream]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[publishexpandedpath]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[attributes]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[foldertypeid]
    Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{1b3ea5dc-
b587-4786-b4ef-bd1dc332aeae}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[{1b3ea5dc-b587-4786-b4ef-bd1dc332aeae}]
    Queries value: HKCR\exefile[nostaticdefaultverb]
    Queries value: HKCR\exefile\shell[]
    Queries value: HKCR\exefile\shell\open[neverdefault]
    Queries value: HKCR\wow6432node\clsid\{1649d1cf-deaf-4a68-abe8-
5c9f68572fd1}\inprocserver32[]
    Queries value: HKCR\exefile\shell\open\command[delegateexecute]
    Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]
    Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[inprocserver32]
    Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[]
    Queries value: HKCR\wow6432node\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[threadingmodel]
    Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[]
    Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
    Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[]
    Queries value: HKCR\wow6432node\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
    Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
    Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[6f21fb21650da014d87426fa0bd8e7f2.exe]
    Queries value: HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
    Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
    Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\zones\0[1806]
    Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[f189f4ab]
    Queries value: HKLM\software\microsoft\sqmclient\windows[studyid]
    Queries value: HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
    Queries value: HKCR\exefile\shell\open\command[command]
    Queries value: HKCR\exefile\shell\open\command[]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
    Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
    Queries value: HKCR\exefile\shell\open[setworkingdirectoryfromtarget]
    Queries value: HKCR\exefile\shell\open[noworkingdirectory]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
    Queries value: HKCR\applications\cmd.exe[immersivebroker]
    Queries value: HKCU\software\microsoft\windows\shell\associations[showtoast]
    Queries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]
    Queries value:

```
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:              HKCU\console[screencolors]
  Queries value:              HKCU\console[popupcolors]
  Queries value:              HKCU\console[insertmode]
  Queries value:              HKCU\console[quickedit]
  Queries value:              HKCU\console[codepage]
  Queries value:              HKCU\console[screenbuffersize]
  Queries value:              HKCU\console[windowsize]
  Queries value:              HKCU\console[windowposition]
  Queries value:              HKCU\console[fontsize]
  Queries value:              HKCU\console[fontfamily]
  Queries value:              HKCU\console[fontweight]
  Queries value:              HKCU\console[facename]
  Queries value:              HKCU\console[cursorsize]
  Queries value:              HKCU\console[historybuffersize]
  Queries value:              HKCU\console[numberofhistorybuffers]
  Queries value:              HKCU\console[historynodup]
  Queries value:              HKCU\console[colortable00]
  Queries value:              HKCU\console[colortable01]
  Queries value:              HKCU\console[colortable02]
  Queries value:              HKCU\console[colortable03]
  Queries value:              HKCU\console[colortable04]
  Queries value:              HKCU\console[colortable05]
  Queries value:              HKCU\console[colortable06]
  Queries value:              HKCU\console[colortable07]
  Queries value:              HKCU\console[colortable08]
  Queries value:              HKCU\console[colortable09]
  Queries value:              HKCU\console[colortable10]
  Queries value:              HKCU\console[colortable11]
  Queries value:              HKCU\console[colortable12]
  Queries value:              HKCU\console[colortable13]
  Queries value:              HKCU\console[colortable14]
  Queries value:              HKCU\console[colortable15]
  Queries value:              HKCU\console[loadconime]
  Queries value:              HKCU\console[extendededitkey]
  Queries value:              HKCU\console[extendededitkeycustom]
  Queries value:              HKCU\console[worddelimiters]
  Queries value:              HKCU\console[trimleadingzeros]
  Queries value:              HKCU\console[enablecolorselection]
  Queries value:              HKCU\console[scrollscale]
  Queries value:              HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  Queries value:              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
  Queries value:              HKLM\software\wow6432node\microsoft\command processor[disableunccheck]
  Queries value:              HKLM\software\wow6432node\microsoft\command processor[enableextensions]
  Queries value:              HKLM\software\wow6432node\microsoft\command processor[delayedexpansion]
  Queries value:              HKLM\software\wow6432node\microsoft\command processor[defaultcolor]
  Queries value:              HKLM\software\wow6432node\microsoft\command processor[completionchar]
  Queries value:              HKLM\software\wow6432node\microsoft\command
processor[pathcompletionchar]
  Queries value:              HKLM\software\wow6432node\microsoft\command processor[autorun]
  Queries value:              HKCU\software\microsoft\command processor[disableunccheck]
  Queries value:              HKCU\software\microsoft\command processor[enableextensions]
  Queries value:              HKCU\software\microsoft\command processor[delayedexpansion]
  Queries value:              HKCU\software\microsoft\command processor[defaultcolor]
  Queries value:              HKCU\software\microsoft\command processor[completionchar]
  Queries value:              HKCU\software\microsoft\command processor[pathcompletionchar]
  Queries value:              HKCU\software\microsoft\command processor[autorun]
  Queries value:              HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[tasklist]
  Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
  Queries value:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
  Queries value:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[logging directory]
  Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
  Queries value:              HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Queries value:              HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:              HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32[]
  Queries value:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
  Queries value:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
```

```
00aa004b2e24}\inprocserver32[inprocserver32]
   Queries value:          HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[]
   Queries value:          HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
   Queries value:          HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32[]
   Queries value:          HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
   Queries value:          HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[inprocserver32]
   Queries value:          HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[]
   Queries value:          HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[threadingmodel]
   Queries value:          HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
   Queries value:          HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
   Queries value:          HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
   Queries value:          HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
   Queries value:          HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
   Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en]
   Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
   Queries value:          HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32[]
   Queries value:          HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
   Queries value:          HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
   Queries value:          HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[]
   Queries value:          HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
   Queries value:          HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-252725d697ca}[]
   Queries value:          HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[inprocserver32]
   Queries value:          HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[]
   Queries value:          HKCR\wow6432node\clsid\{e7d35cfa-348b-485e-b524-
252725d697ca}\inprocserver32[threadingmodel]
   Queries value:          HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32[]
   Queries value:          HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
   Queries value:          HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
   Queries value:          HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[]
   Queries value:          HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
   Queries value:          HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32[]
   Queries value:          HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32[]
   Queries value:          HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-00c04fb68820}[]
   Queries value:          HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprocserver32[inprocserver32]
   Queries value:          HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprocserver32[]
   Queries value:          HKCR\wow6432node\clsid\{eb87e1bd-3233-11d2-aec9-
00c04fb68820}\inprocserver32[threadingmodel]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
   Value changes:          HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
```