Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2423
Risk Level:	6
Date Processed:	2016-02-22 05:28:19 (UTC)
Processing Time:	61.4 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"

Sample ID:	619
Type:	basic
Owner:	admin
Label:	81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui
File Size:	286720 bytes
MD5:	6f2159e72e7ab7b02e18211ecbed7dd3
SHA256:	81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
Description:	None

Pattern Matching Results

1	YARA score 1
6	Modifies registry autorun entries
3	HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]
6	Dumps and runs batch script
5	Adds autostart object
4	Terminates process under Windows subfolder

Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable

Process/Thread Events

Creates process:	C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe ["C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe"]
Creates process:	C:\Users\Public\WinJab\winjab.exe ["C:\Users\Public\WinJab\winjab.exe"]
Creates process:	C:\Windows\system32\cmd.exe [cmd /c C:\Users\Public\1.bat]
Terminates process:	C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
Terminates process:	C:\Windows\System32\cmd.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates mutex:	\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!roaming!microsoft!windows!cookies!
Creates mutex:	\Sessions\1\BaseNamedObjects\c:!users!admin!appdata!local!microsoft!windows!history!history.ie5!
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetStartupMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates event:	\Sessions\1\BaseNamedObjects\OleDfRootA335511A244DB07D
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{36dfc21c-93c8-485b-9ebf-9a3c5393a6c3}
Creates event:	\BaseNamedObjects\ConsoleEvent-0x00000A28
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?81F686A320DBEC38A90D64C98861F8DDAC8BFDAA7F1AD04A8A33961283E00A22.EXE
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?USERS?PUBLIC?WINJAB?WINJAB.EXE

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\~DF220BF13BEA5BF4AC.TMP
Creates:	C:\Users\Public\WinJab
Creates:	C:\Users\Public\WinJab\winjab.exe
Creates:	C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
Creates:	C:\Users\Public\1.bat
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\81F686A320DBEC38A90D64C98861F-9845A13B.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\MSVBVM60.DLL

```
  Opens:                  C:\Windows\System32\msvbvm60.dll
  Opens:                  C:\Windows\System32\sechost.dll
  Opens:                  C:\Windows\System32\imm32.dll
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\System32\rpcss.dll
  Opens:                  C:\windows\temp\CRYPTBASE.dll
  Opens:                  C:\Windows\System32\cryptbase.dll
  Opens:                  C:\Windows\System32\uxtheme.dll
  Opens:
C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe.cfg
  Opens:                  C:\windows\temp\SXS.DLL
  Opens:                  C:\Windows\System32\sxs.dll
  Opens:                  C:\Windows\System32\C_932.NLS
  Opens:                  C:\Windows\System32\C_949.NLS
  Opens:                  C:\Windows\System32\C_950.NLS
  Opens:                  C:\Windows\System32\C_936.NLS
  Opens:                  C:\windows\temp\winmm.dll
  Opens:                  C:\Windows\System32\winmm.dll
  Opens:                  C:\Windows\Fonts\sserife.fon
  Opens:                  C:\windows\temp\CRYPTSP.dll
  Opens:                  C:\Windows\System32\cryptsp.dll
  Opens:                  C:\Windows\System32\rsaenh.dll
  Opens:                  C:\windows\temp\dwmapi.dll
  Opens:                  C:\Windows\System32\dwmapi.dll
  Opens:                  C:\Windows\Fonts\verdanab.ttf
  Opens:                  C:\Windows\system32\uxtheme.dll.Config
  Opens:
C:\windows\temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe.Local\
  Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
  Opens:                  C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
  Opens:                  C:\Windows\WindowsShell.Manifest
  Opens:                  C:\Windows\Fonts\lucon.ttf
  Opens:                  C:\Windows\System32\ieframe.dll
  Opens:                  C:\Windows\System32\oleacc.dll
  Opens:                  C:\windows\temp\OLEACCRC.DLL
  Opens:                  C:\Windows\System32\oleaccrc.dll
  Opens:                  C:\Windows\Fonts\verdana.ttf
  Opens:                  C:\Windows\System32\asycfilt.dll
  Opens:                  C:\Windows\System32\winhttp.dll
  Opens:                  C:\Windows\System32\webio.dll
  Opens:                  C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:                  C:\windows\temp\SspiCli.dll
  Opens:                  C:\Windows\System32\sspicli.dll
  Opens:                  C:\windows\temp\credssp.dll
  Opens:                  C:\Windows\System32\credssp.dll
  Opens:                  C:\Windows\System32\mswsock.dll
  Opens:                  C:\Windows\System32\wshqos.dll
  Opens:                  C:\windows\temp\wshtcpip.DLL
  Opens:                  C:\Windows\System32\WSHTCPIP.DLL
  Opens:                  C:\windows\temp\wship6.dll
  Opens:                  C:\Windows\System32\wship6.dll
  Opens:                  C:\windows\temp\DNSAPI.dll
  Opens:                  C:\Windows\System32\dnsapi.dll
  Opens:                  C:\windows\temp\IPHLPAPI.DLL
  Opens:                  C:\Windows\System32\IPHLPAPI.DLL
  Opens:                  C:\windows\temp\WINNSI.DLL
  Opens:                  C:\Windows\System32\winnsi.dll
  Opens:                  C:\windows\temp\dhcpcsvc6.DLL
  Opens:                  C:\Windows\System32\dhcpcsvc6.dll
  Opens:                  C:\windows\temp\dhcpcsvc.DLL
  Opens:                  C:\Windows\System32\dhcpcsvc.dll
  Opens:                  C:\windows\temp\rasadhlp.dll
  Opens:                  C:\Windows\System32\rasadhlp.dll
  Opens:                  C:\Windows\System32\drivers\etc\hosts
  Opens:                  C:\Windows\System32\FWPUCLNT.DLL
  Opens:                  C:\Windows\System32\scrrun.dll
  Opens:                  C:\Windows\System32\version.dll
  Opens:                  C:\Users\Public\WinJab\
  Opens:                  C:\Users\Public\WinJab
  Opens:                  C:\Users\Public\WinJab\winjab.exe
  Opens:                  C:\Windows\Temp
  Opens:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
  Opens:                  C:\Windows\System32\apphelp.dll
  Opens:                  C:\Windows\AppPatch\sysmain.sdb
  Opens:                  C:\
  Opens:                  C:\Users
  Opens:                  C:\Users\Public
  Opens:                  C:\Users\Public\WinJab\ui\SwDRM.dll
  Opens:                  C:\Windows\Prefetch\WINJAB.EXE-59459BCE.pf
  Opens:                  C:\Users\Public\WinJab\MSVBVM60.DLL
  Opens:                  C:\Users\Public\WinJab\CRYPTBASE.dll
  Opens:                  C:\Users\Public\WinJab\winjab.exe.cfg
  Opens:                  C:\Users\Public\WinJab\SXS.DLL
  Opens:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
  Opens:                  C:\Users\Public\1.bat
  Opens:                  C:\windows\temp\cmd.exe
  Opens:                  C:\Windows\System32\cmd.exe
  Opens:                  C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Opens:                  C:
  Opens:                  C:\Program Files
  Opens:                   C:\Windows\System32\wininet.dll
  Opens:                   C:\Program Files\Adobe
  Opens:                   C:\Program Files\Adobe\Reader 9.0
  Opens:                   C:\Program Files\Adobe\Reader 9.0\Reader
  Opens:                   C:\Windows
  Opens:                   C:\Windows\Branding
  Opens:                   C:\Windows\Branding\Basebrd
  Opens:                   C:\Windows\Branding\Basebrd\en-US
  Opens:                   C:\Windows\Globalization
  Opens:                   C:\Windows\Globalization\Sorting
  Opens:                   C:\Windows\System32\en-US
  Opens:                   C:\Windows\System32\ntdll.dll
  Opens:                   C:\Windows\System32\kernel32.dll
  Opens:                   C:\Windows\System32\apisetschema.dll
  Opens:                   C:\Windows\System32\KernelBase.dll
  Opens:                   C:\Windows\System32\locale.nls
  Opens:                   C:\Windows\System32\msvcrt.dll
  Opens:                   C:\Windows\System32\winbrand.dll
  Opens:                   C:\Windows\System32\user32.dll
  Opens:                   C:\Windows\System32\gdi32.dll
  Opens:                   C:\Windows\System32\lpk.dll
  Opens:                   C:\Windows\System32\usp10.dll
  Opens:                   C:\Windows\System32\msctf.dll
  Opens:                   C:\Windows\System32\en-US\cmd.exe.mui
  Opens:                   C:\Windows\Branding\Basebrd\basebrd.dll
  Opens:                   C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
  Opens:                   C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
  Opens:                   C:\windows\temp\profapi.dll
  Opens:                   C:\Windows\System32\profapi.dll
  Opens:                   C:\Users\Admin
  Opens:                   C:\Users\Admin\AppData\Local
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
  Opens:                   C:\Users\Admin\AppData\Roaming
  Opens:                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
  Opens:                   C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
  Opens:                   C:\Users\Public\1.bat\
  Opens:                   C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:                   C:\windows\temp\ntmarta.dll
  Opens:                   C:\Windows\System32\ntmarta.dll
  Opens:                   C:\Windows\WINHELP.INI
  Opens:                   C:\Windows\system32\.HLP
  Opens:                   C:\Windows\Help\.HLP
  Opens:                   C:\Users\Admin\AppData\Local\Temp\~DF220BF13BEA5BF4AC.TMP
  Opens:                   C:\Users\Public\WinJab\winmm.dll
  Writes to:               C:\Users\Public\WinJab\winjab.exe
  Writes to:               C:\Users\Public\1.bat
  Reads from:              C:\Windows\System32\drivers\etc\hosts
  Reads from:              C:\Windows\System32\scrrun.dll
  Reads from:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
  Reads from:              C:\Users\Public\WinJab\winjab.exe
  Reads from:              C:\Users\Public\1.bat
  Reads from:              C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Deletes:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22
  Deletes:
C:\Windows\Temp\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
  Deletes:                 C:\Users\Admin\AppData\Local\Temp\~DF220BF13BEA5BF4AC.TMP
  Deletes:                 C:\Users\Public\1.bat
```

Network Events

```
  DNS query:               muzanaczekanie.pl
  DNS response:            muzanaczekanie.pl ⇒ 188.165.23.155
  Connects to:             188.165.23.155:80
  Sends data to:           8.8.8.8:53
  Sends data to:           muzanaczekanie.pl:80 (188.165.23.155)
  Receives data from:      8.8.8.8:53
  Receives data from:      muzanaczekanie.pl:80 (188.165.23.155)
```

Windows Registry Events

```
  Creates key:             HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:             HKCU\software\microsoft\windows\currentversion\run
  Creates key:             HKCU\software\vb and vba program settings\clock\sdata
  Creates key:             HKCU\software
  Creates key:             HKCU\software\vb and vba program settings
  Creates key:             HKCU\software\vb and vba program settings\clock
  Creates key:             HKCU\software\microsoft\windows\currentversion\internet settings
  Deletes value:           HKCU\software\microsoft\internet
```

```
explorer\lowregistry[addtofavoritesinitialselection]
  Deletes value:              HKCU\software\microsoft\internet
explorer\lowregistry[addtofeedsinitialselection]
  Opens key:                  HKLM\system\currentcontrolset\control\session manager
  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\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKCU\
  Opens key:                  HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                  HKLM\software\policies\microsoft\mui\settings
  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\microsoft\windows\currentversion\sidebyside
  Opens key:                  HKLM\system\currentcontrolset\control\nls\sorting\versions
  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\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\
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                  HKLM\software\microsoft\ole
  Opens key:                  HKLM\software\microsoft\ole\tracing
  Opens key:                  HKLM\software\microsoft\oleaut
  Opens key:                  HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                  HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                  HKLM\system\currentcontrolset\control\nls\locale
  Opens key:                  HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:                  HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:                  HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:                  HKLM\system\currentcontrolset\control\nls\codepage
  Opens key:                  HKLM\software\microsoft\vba\monitors
  Opens key:
HKLM\software\microsoft\ctf\compatibility\81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe
  Opens key:                  HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
  Opens key:                  HKLM\software\microsoft\ctf\
  Opens key:                  HKLM\software\microsoft\ctf\knownclasses
  Opens key:                  HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  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\policies\microsoft\cryptography
  Opens key:                  HKLM\software\microsoft\cryptography
  Opens key:                  HKLM\software\microsoft\cryptography\offload
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                  HKCU\software\classes\
  Opens key:                  HKLM\software\microsoft\com3
  Opens key:                  HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                  HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
  Opens key:                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:                  HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\progid
  Opens key:                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid
  Opens key:                  HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
  Opens key:                  HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
  Opens key:                  HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler
  Opens key:                  HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler
  Opens key:                  HKLM\software\microsoft\rpc
  Opens key:                  HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                  HKLM\system\setup
  Opens key:                  HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                  HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                  HKLM\software\microsoft\sqmclient\windows
  Opens key:                  HKCU\software\classes\clsid\{00021401-0000-0000-c000-000000000046}
  Opens key:                  HKCR\clsid\{00021401-0000-0000-c000-000000000046}
  Opens key:                  HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\treatas
  Opens key:                  HKCR\clsid\{00021401-0000-0000-c000-000000000046}\treatas
  Opens key:                  HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\progid
  Opens key:                  HKCR\clsid\{00021401-0000-0000-c000-000000000046}\progid
  Opens key:                  HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                  HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00021401-0000-0000-c000-
000000000046}\inprochandler
  Opens key:                HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprochandler
  Opens key:                HKLM\system\currentcontrolset\services\crypt32
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKCU\software\policies\microsoft\control
panel\international\calendars\twodigityearmax
  Opens key:                HKCU\control panel\international\calendars\twodigityearmax
  Opens key:                HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}
  Opens key:                HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}
  Opens key:                HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\treatas
  Opens key:                HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\treatas
  Opens key:                HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\progid
  Opens key:                HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\progid
  Opens key:                HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32
  Opens key:                HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprochandler32
  Opens key:                HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprochandler
  Opens key:                HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprochandler
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
  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\07a0e1d6
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  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\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  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\system\currentcontrolset\control\cmf\config
  Opens key:                        HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli
  Opens key:                        HKLM\system\currentcontrolset\control\securityproviders
  Opens key:                        HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                        HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll
  Opens key:                        HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  Opens key:                        HKLM\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                        HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                        HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                        HKLM\system\currentcontrolset\services\psched\parameters\winsock
  Opens key:                        HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
  Opens key:                        HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                        HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                        HKLM\system\currentcontrolset\services\dns
  Opens key:                        HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:                        HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:                        HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:                        HKLM\software\policies\microsoft\system\dnsclient
  Opens key:                        HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:                        HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:                        HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
  Opens key:                        HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                        HKCU\software\classes\scripting.filesystemobject
  Opens key:                        HKCR\scripting.filesystemobject
  Opens key:                        HKCU\software\classes\scripting.filesystemobject\clsid
  Opens key:                        HKCR\scripting.filesystemobject\clsid
  Opens key:                        HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key:                        HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}
  Opens key:                        HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\treatas
  Opens key:                        HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\treatas
  Opens key:                        HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\progid
  Opens key:                        HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\progid
  Opens key:                        HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32
  Opens key:                        HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32
  Opens key:                        HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler32
  Opens key:                        HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler32
  Opens key:                        HKCU\software\classes\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprochandler
  Opens key:                        HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprochandler
  Opens key:                        HKCU\software\classes\typelib
  Opens key:                        HKCR\typelib
  Opens key:                        HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
  Opens key:                        HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}
  Opens key:                        HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
  Opens key:                        HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0
  Opens key:                        HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-
00a0c9054228}\1.0\0
  Opens key:                        HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0
  Opens key:                        HKCU\software\classes\typelib\{420b2830-e718-11cf-893d-
00a0c9054228}\1.0\0\win32
  Opens key:                        HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32
  Opens key:                        HKCU\software\vb and vba program settings\clock\sdata
  Opens key:                        HKLM\software\policies\microsoft\windows\system
  Opens key:                        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winjab.exe
  Opens key:                        HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                        HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                        HKLM\software\policies\microsoft\windows\appcompat
  Opens key:                        HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                        HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\winjab.exe
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\1.bat
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies
  Opens key:                HKCU\software\policies
  Opens key:                HKCU\software
  Opens key:                HKLM\software
  Opens key:                HKLM\software\policies\microsoft\internet explorer
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}
  Opens key:
HKLM\software\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:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\policies\microsoft\windows\explorer
  Opens key:                HKCU\software\policies\microsoft\windows\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}\propertybag
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}\propertybag
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
  Opens key:
HKLM\software\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\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}\propertybag
  Opens key:                HKCU\software\policies\microsoft\windows\system
  Opens key:                HKLM\software\microsoft\command processor
  Opens key:                HKCU\software\microsoft\command processor
  Opens key:                HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
```

```
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKLM\system\currentcontrolset\control\srp\\gp\
  Opens key:                HKLM\system\currentcontrolset\control\srp\\gp
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKLM\software\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\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  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_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKLM\software\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\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKLM\software\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\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                HKLM\software\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\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\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\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\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                HKLM\software\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\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\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:                HKLM\system\currentcontrolset\control\lsa\accessproviders
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\cache
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\cache
  Opens key:                HKCU\software\microsoft\internet explorer\lowregistry
  Opens key:                HKLM\software\microsoft\windows
  Opens key:                HKLM\software\microsoft\windows\html help
  Opens key:                HKLM\software\microsoft\windows\help
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\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\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[932]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[949]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[950]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage[936]
  Queries value:            HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:              HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  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:              HKLM\software\microsoft\com3[com+enabled]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\progid[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
  Queries value:              HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
  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\sqmclient\windows[ceipenable]
  Queries value:              HKCR\clsid\{00021401-0000-0000-c000-000000000046}\progid[]
  Queries value:              HKCR\clsid\{00021401-0000-0000-c000-000000000046}[]
  Queries value:              HKCR\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{00021401-0000-0000-c000-000000000046}\inprocserver32[]
  Queries value:              HKCR\clsid\{00021401-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
  Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
  Queries value:              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\progid[]
  Queries value:              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}[]
  Queries value:              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-66779b670495}\inprocserver32[]
  Queries value:              HKCR\clsid\{2087c2f4-2cef-4953-a8ab-
66779b670495}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing[enabled]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp[disablebranchcache]
  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\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[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\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:          HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignaturedll]
  Queries value:
HKLM\system\currentcontrolset\control\lsaextensionconfig\sspicli[checksignatureroutine]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[name]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[capabilities]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[rpcid]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[version]
  Queries value:          HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\credssp.dll[tokensize]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
  Queries value:          HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
  Queries value:          HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[helperdllname]
  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[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[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\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  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\winsock[helperdllname]
  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:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:            HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enablemulticast]
  Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:              HKCR\scripting.filesystemobject\clsid[]
  Queries value:              HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\progid[]
  Queries value:              HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}[]
  Queries value:              HKCR\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{0d43fe01-f093-11cf-8940-00a0c9054228}\inprocserver32[]
  Queries value:              HKCR\clsid\{0d43fe01-f093-11cf-8940-
00a0c9054228}\inprocserver32[threadingmodel]
  Queries value:              HKCR\typelib\{420b2830-e718-11cf-893d-00a0c9054228}\1.0\0\win32[]
  Queries value:
HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]
  Queries value:              HKLM\software\policies\microsoft\windows\system[copyfilechunksize]
  Queries value:              HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\users\public\winjab\winjab.exe]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[winjab]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\users\public\1.bat]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
  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[disablepassport]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
  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\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
```

```
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[initfolderhandler]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[foldertypeid]
  Queries value:
HKLM\software\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\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[foldertypeid]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[initfolderhandler]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002[profileimagepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[icon]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[security]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[streamresource]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[streamresourcetype]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[localredirectonly]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[roamable]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[precreate]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[stream]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}[foldertypeid]
  Queries value:
HKLM\software\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\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[category]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[name]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parentfolder]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[description]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[relativepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[parsingname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[infotip]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}[localizedname]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
```

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

```
a781-5a1130a75963}[publishexpandedpath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[attributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[foldertypeid]
  Queries value:
HKLM\software\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[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
  Queries value:            HKLM\software\microsoft\command processor[disableunccheck]
  Queries value:            HKLM\software\microsoft\command processor[enableextensions]
  Queries value:            HKLM\software\microsoft\command processor[delayedexpansion]
  Queries value:            HKLM\software\microsoft\command processor[defaultcolor]
  Queries value:            HKLM\software\microsoft\command processor[completionchar]
  Queries value:            HKLM\software\microsoft\command processor[pathcompletionchar]
  Queries value:            HKLM\software\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\policies\microsoft\windows\safer\codeidentifiers[levels]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[saferflags]
  Queries value:            HKLM\system\currentcontrolset\control\srp\gp[rulecount]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  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[mbcsapiforcrack]
  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\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\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKLM\software\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\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKLM\software\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\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:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[81f686a320dbec38a90d64c98861f8ddac8bfdaa7f1ad04a8a33961283e00a22.exe]
  Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKLM\software\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\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
```

```
settings[enablehttptrace]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  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\system\currentcontrolset\control\lsa\accessproviders[martaextension]
  Queries value:              HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:              HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
  Queries value:              HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
  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:              HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\cache[persistent]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\cache[persistent]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\cache[persistent]
  Queries value:              HKLM\software\microsoft\windows\html help[.hlp]
  Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\run[wincl]
  Sets/Creates value:         HKCU\software\vb and vba program settings\clock\sdata[s]
```