Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	766
Risk Level:	10
Date Processed:	2016-05-18 10:35:49 (UTC)
Processing Time:	80.91 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\857bd61a8241ac81385ee957d8137887.exe"
Sample ID:	3314
Type:	basic
Owner:	admin
Label:	857bd61a8241ac81385ee957d8137887
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	184832 bytes
MD5:	857bd61a8241ac81385ee957d8137887
SHA256:	efed61ac534b30cf6837dea448b72c43ec008f31273c445440a934aa5246ba2f
Description:	None

Pattern Matching Results

5	PE: Contains compressed section
3	HTTP connection - response code 200 (success)
10	Creates malicious events: Cycbot [Backdoor]
4	Checks whether debugger is present
3	Long sleep detected

Process/Thread Events

Creates process:	C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe ["C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe"]
Creates process:	C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe [C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe startC:\Program Files (x86)\LP\6930\027.exe%C:\Program Files (x86)\LP\6930]
Creates process:	C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe [C:\windows\temp\857bd61a8241ac81385ee957d8137887.exe startC:\Users\Admin\AppData\Roaming\0CE74\B5469.exe%C:\Users\Admin\AppData\Roaming\0CE74]
Terminates process:	C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\{5D92BB9F-9A66-458f-ACA4-66172A7016D4}
Creates mutex:	\Sessions\1\BaseNamedObjects\{4D92BB9F-9A66-458f-ACA4-66172A7016D4}
Creates mutex:	\Sessions\1\BaseNamedObjects\{61B98B86-5F44-42b3-BCA1-33904B067B81}
Creates mutex:	\Sessions\1\BaseNamedObjects\{B16C7E24-B3B8-4962-BF5E-4B33FD2DFE78}
Creates mutex:	\Sessions\1\BaseNamedObjects\{B37C48AF-B05C-4520-8B38-2FE181D5DC78}
Creates mutex:	\Sessions\1\BaseNamedObjects\{0ECE180F-6E9E-4FA6-A154-6876D9DB8906}
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 mutex:	\Sessions\1\BaseNamedObjects\4A3282FEF482C0F79E1
Creates event:	\Sessions\1\BaseNamedObjects\{6B985724-623F-492e-B0D6-C9715ADE853B}
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{3947d672-e600-4192-bf94-ce35ec765800}

File System Events

Creates:	C:\Program Files (x86)
Creates:	C:\Program Files (x86)\74E66
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\0CE74
Creates:	C:\Users\Admin\AppData\Roaming\0CE74\4E66.CE7
Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Program Files (x86)\LP
Creates:	C:\Program Files (x86)\LP\6930

```
  Creates:               C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Creates:               C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                 C:\Windows\Prefetch\857BD61A8241AC81385EE957D8137-5577336B.pf
  Opens:                 C:\Windows
  Opens:                 C:\Windows\System32\wow64.dll
  Opens:                 C:\Windows\System32\wow64win.dll
  Opens:                 C:\Windows\System32\wow64cpu.dll
  Opens:                 C:\Windows\system32\wow64log.dll
  Opens:                 C:\Windows\SysWOW64
  Opens:                 C:\windows\temp\oleacc.dll
  Opens:                 C:\Windows\SysWOW64\oleacc.dll
  Opens:                 C:\Windows\SysWOW64\sechost.dll
  Opens:                 C:\windows\temp\MSIMG32.DLL
  Opens:                 C:\Windows\SysWOW64\msimg32.dll
  Opens:                 C:\Windows\SysWOW64\imm32.dll
  Opens:                 C:\windows\temp\OLEACCRC.DLL
  Opens:                 C:\Windows\SysWOW64\oleaccrc.dll
  Opens:                 C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                 C:\windows\temp\_CÂuVirtualProtect.DLL
  Opens:                 C:\Windows\SysWOW64\_CÂuVirtualProtect.DLL
  Opens:                 C:\Windows\system\_CÂuVirtualProtect.DLL
  Opens:                 C:\Windows\_CÂuVirtualProtect.DLL
  Opens:                 C:\Windows\SysWOW64\Wbem\_CÂuVirtualProtect.DLL
  Opens:                 C:\Windows\SysWOW64\WindowsPowerShell\v1.0\_CÂuVirtualProtect.DLL
  Opens:                 C:\windows\temp\apphelp.dll
  Opens:                 C:\Windows\SysWOW64\apphelp.dll
  Opens:                 C:\windows\temp\RASAPI32.dll
  Opens:                 C:\Windows\SysWOW64\rasapi32.dll
  Opens:                 C:\windows\temp\rasman.dll
  Opens:                 C:\Windows\SysWOW64\rasman.dll
  Opens:                 C:\windows\temp\WINHTTP.dll
  Opens:                 C:\Windows\SysWOW64\winhttp.dll
  Opens:                 C:\windows\temp\webio.dll
  Opens:                 C:\Windows\SysWOW64\webio.dll
  Opens:                 C:\
  Opens:                 C:\Program Files (x86)
  Opens:                 C:\Program Files (x86)\74E66
  Opens:                 C:\Users\Admin\AppData\Roaming\0CE74
  Opens:                 C:\Users\Admin\AppData\Roaming\0CE74\4E66.CE7
  Opens:                 C:\Windows\SysWOW64\mswsock.dll
  Opens:                 C:\Windows\SysWOW64\WSHTCPIP.DLL
  Opens:                 C:\Windows\SysWOW64\wininet.dll
  Opens:                 C:\windows\temp\857bd61a8241ac81385ee957d8137887.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\temp\profapi.dll
  Opens:                 C:\Windows\SysWOW64\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:\Program Files (x86)\LP\6930
  Opens:                 C:\Windows\Temp
  Opens:                 C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe
  Opens:                 C:\Windows\SysWOW64\wship6.dll
  Opens:                 C:\Users\Admin\AppData\Roaming
  Opens:                 C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
  Opens:                 C:\Windows\SysWOW64\rpcss.dll
  Opens:                 C:\Windows\SysWOW64\uxtheme.dll
  Opens:                 C:\windows\temp\DNSAPI.dll
  Opens:                 C:\Windows\SysWOW64\dnsapi.dll
  Opens:                 C:\Users\Admin\AppData\Roaming\Cloud AV 2012\ahst.lni
  Opens:                 C:\windows\temp\IPHLPAPI.DLL
  Opens:                 C:\Windows\SysWOW64\IPHLPAPI.DLL
  Opens:                 C:\windows\temp\WINNSI.DLL
  Opens:                 C:\Windows\SysWOW64\winnsi.dll
  Opens:                 C:\Users\Admin\AppData\Local\Microsoft\Windows\History
  Opens:                 C:\Windows\SysWOW64\FirewallAPI.dll
  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\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
  Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
  Opens:                  C:\Windows\SysWOW64\version.dll
  Opens:                  C:\windows\temp\dhcpcsvc6.DLL
  Opens:                  C:\Windows\SysWOW64\dhcpcsvc6.dll
  Opens:                  C:\windows\temp\dhcpcsvc.DLL
  Opens:                  C:\Windows\SysWOW64\dhcpcsvc.dll
  Opens:                  C:\windows\temp\rasadhlp.dll
  Opens:                  C:\Windows\SysWOW64\rasadhlp.dll
  Opens:                  C:\Windows\System32\drivers\etc\hosts
  Opens:                  C:\windows\temp\rtutils.dll
  Opens:                  C:\Windows\SysWOW64\rtutils.dll
  Opens:                  C:\Program
  Opens:                  C:\Program.exe
  Opens:                  C:\Program Files
  Opens:                  C:\Program Files (x86)\LP\6930\027.exe
  Opens:                  C:\Program Files (x86)\LP\6930\027.exe.exe
  Opens:                  C:\ProgramData\Microsoft\Network\Connections\Pbk\
  Opens:                  C:\Windows\SysWOW64\ras
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
  Opens:                  C:\windows\temp\sensapi.dll
  Opens:                  C:\Windows\SysWOW64\SensApi.dll
  Opens:                  C:\Users\Admin\AppData\Roaming\Mozilla\
  Opens:                  C:\Users\Admin\AppData\Roaming\Opera\
  Opens:                  C:\Windows\SysWOW64\wbem\wbemprox.dll
  Opens:                  C:\Windows\SysWOW64\wbem\wbemcomn.dll
  Opens:                  C:\Windows\SysWOW64\wbemcomn.dll
  Opens:                  C:\Windows\SysWOW64\wbem\Logs
  Opens:                  C:\windows\temp\CRYPTSP.dll
  Opens:                  C:\Windows\SysWOW64\cryptsp.dll
  Opens:                  C:\Windows\SysWOW64\rsaenh.dll
  Opens:                  C:\windows\temp\RpcRtRemote.dll
  Opens:                  C:\Windows\SysWOW64\RpcRtRemote.dll
  Opens:                  C:\Windows\SysWOW64\wbem\wbemsvc.dll
  Opens:                  C:\Windows\SysWOW64\wbem\fastprox.dll
  Opens:                  C:\Windows\SysWOW64\wbem\NTDSAPI.dll
  Opens:                  C:\Windows\SysWOW64\ntdsapi.dll
  Opens:                  C:\Windows\SysWOW64\FWPUCLNT.DLL
  Opens:                  C:\Users\Admin\AppData\Roaming\0CE74\B5469.exe
  Opens:                  C:\Users\Admin\AppData\Roaming\0CE74\B5469.exe.exe
  Opens:                  C:\Windows\SysWOW64\nlaapi.dll
  Opens:                  C:\Windows\SysWOW64\NapiNSP.dll
  Opens:                  C:\Windows\SysWOW64\pnrpnsp.dll
  Opens:                  C:\Windows\SysWOW64\winrnr.dll
  Writes to:              C:\Users\Admin\AppData\Roaming\0CE74\4E66.CE7
  Reads from:             C:\Windows\Temp\857bd61a8241ac81385ee957d8137887.exe
  Reads from:             C:\Windows\System32\drivers\etc\hosts
```

Network Events

```
  DNS query:              cdn.adventofdeception.com
  DNS query:              krq.enotusfed.com
  DNS query:              jybeu.kupinosis.com
  DNS query:              www.google.com
  DNS query:              ncd.kupinosis.com
  DNS query:              xprstats.com
  DNS query:              ocsp.verisign.com
  DNS response:           www.google.com ⇒ 58.26.8.109
  DNS response:           www.google.com ⇒ 58.26.8.99
  DNS response:           www.google.com ⇒ 58.26.8.89
  DNS response:           www.google.com ⇒ 58.26.8.94
  DNS response:           www.google.com ⇒ 58.26.8.103
  DNS response:           www.google.com ⇒ 58.26.8.98
  DNS response:           www.google.com ⇒ 58.26.8.108
  DNS response:           www.google.com ⇒ 58.26.8.113
  DNS response:           www.google.com ⇒ 58.26.8.84
  DNS response:           www.google.com ⇒ 58.26.8.93
  DNS response:           www.google.com ⇒ 58.26.8.119
  DNS response:           www.google.com ⇒ 58.26.8.118
  DNS response:           www.google.com ⇒ 58.26.8.104
  DNS response:           www.google.com ⇒ 58.26.8.114
  DNS response:           www.google.com ⇒ 58.26.8.123
  DNS response:           www.google.com ⇒ 58.26.8.88
  DNS response:           e8218.dscb1.akamaiedge.net ⇒ 23.15.155.27
  Connects to:            58.26.8.109:80
  Connects to:            23.15.155.27:80
  Sends data to:          8.8.8.8:53
  Sends data to:          www.google.com:80 (58.26.8.109)
  Sends data to:          e8218.dscb1.akamaiedge.net:80 (23.15.155.27)
  Sends data to:          127.0.0.1:49162
  Sends data to:          127.0.0.1:49164
  Receives data from:     8.8.8.8:53
  Receives data from:     www.google.com:80 (58.26.8.109)
  Receives data from:      127.0.0.1:49162
  Receives data from:      e8218.dscb1.akamaiedge.net:80 (23.15.155.27)
  Receives data from:      127.0.0.1:49164
```

Windows Registry Events

```
  Creates key:             HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:             HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:             HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Creates key:             HKLM\software\wow6432node\microsoft\tracing
  Creates key:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32
  Creates key:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs
  Creates key:             HKLM\software\wow6432node\microsoft\wbem\cimom
  Deletes value:           HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Deletes value:           HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:               HKLM\system\currentcontrolset\control\session manager
  Opens key:               HKLM\software\microsoft\wow64
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:               HKLM\system\currentcontrolset\control\terminal server
  Opens key:               HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:               HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:               HKLM\system\currentcontrolset\control\nls\language
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:               HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:               HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:               HKLM\software\policies\microsoft\mui\settings
  Opens key:               HKCU\
  Opens key:               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:               HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:               HKCU\software\policies\microsoft\control panel\desktop
  Opens key:               HKCU\control panel\desktop\languageconfiguration
  Opens key:               HKCU\control panel\desktop
  Opens key:               HKCU\control panel\desktop\muicached
  Opens key:               HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:               HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:               HKLM\
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:               HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:               HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:               HKLM\software\wow6432node\microsoft\ole
  Opens key:               HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:               HKLM\software\microsoft\ole\tracing
  Opens key:               HKLM\software\wow6432node\microsoft\oleaut
  Opens key:               HKCU\software\classes\
  Opens key:               HKCU\software\classes\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
  Opens key:               HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
00aa00389b71}\proxystubclsid32
  Opens key:               HKLM\system\currentcontrolset\services\crypt32
  Opens key:               HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
  Opens key:               HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:               HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:               HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:               HKLM\software\wow6432node\microsoft\rpc
  Opens key:               HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:               HKLM\system\setup
  Opens key:               HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
  Opens key:               HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:               HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                 HKLM\software\microsoft\sqmclient\windows
  Opens key:                 HKLM\software\microsoft\rpc
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}\propertybag
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}\propertybag
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfoldersettings
  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\1b6cd5d7
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
  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\services\winsock\parameters
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                 HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                 HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:                 HKLM\software\wow6432node\policies
  Opens key:                 HKCU\software\policies
  Opens key:                 HKCU\software
  Opens key:                 HKLM\software\wow6432node
  Opens key:                 HKLM\software\wow6432node\policies\microsoft\internet explorer
  Opens key:                HKLM\software\policies\microsoft\internet explorer
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\wow6432node\policies\microsoft\internet
explorer\main\featurecontrol
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol
  Opens key:                HKLM\software\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}\propertybag
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows\explorer
  Opens key:                HKLM\software\policies\microsoft\windows\explorer
  Opens key:                HKCU\software\policies\microsoft\windows\explorer
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}\propertybag
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-
0e22-4760-9afe-ea3317b67173}\propertybag
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
980053277-1733835069-2361817685-1001
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}\propertybag
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\857bd61a8241ac81385ee957d8137887.exe
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows\appcompat
  Opens key:                HKLM\software\policies\microsoft\windows\appcompat
  Opens key:                HKCU\software\microsoft\windows nt\currentversion
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\857bd61a8241ac81385ee957d8137887.exe
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}\propertybag
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}
  Opens key:                HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\treatas
  Opens key:                HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\progid
  Opens key:                HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid
  Opens key:                HKLM\software\wow6432node\policies\microsoft\system\dnsclient
  Opens key:                HKLM\software\policies\microsoft\system\dnsclient
  Opens key:                HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}\propertybag
  Opens key:                HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprochandler
  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\wow6432node\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                HKLM\system\currentcontrolset\control\sqmservicelist
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings\5.0\cache
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
```

```
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                  HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:                  HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
  Opens key:                  HKLM\software\wow6432node\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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  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\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                  HKLM\system\currentcontrolset\services\dns
  Opens key:                  HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
  Opens key:                  HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
  Opens key:                  HKU\
  Opens key:                  HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}
  Opens key:                  HKLM\software\wow6432node\microsoft\rpc\securityservice
  Opens key:                  HKLM\software\microsoft\rpc\securityservice
  Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-
127795cce47a}
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-
65fee5bae0b1}
  Opens key:                  HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                  HKLM\software\wow6432node\microsoft\rpc\extensions
  Opens key:                  HKLM\software\microsoft\rpc\extensions
  Opens key:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32
  Opens key:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs
  Opens key:                  HKLM\software\wow6432node\microsoft\windows
nt\currentversion\profilelist
  Opens key:                  HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:                  HKLM\software\microsoft\sqmclient\windows\disabledsessions\
  Opens key:                  HKCU\software\classes\appid\857bd61a8241ac81385ee957d8137887.exe
  Opens key:                  HKCR\appid\857bd61a8241ac81385ee957d8137887.exe
  Opens key:                  HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}
  Opens key:                HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\treatas
  Opens key:                HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\progid
  Opens key:                HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
  Opens key:                HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:                HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\progid
  Opens key:                HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid
  Opens key:                HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}
  Opens key:                HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\treatas
  Opens key:                HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\progid
  Opens key:                HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\progid
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
  Opens key:                HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
  Opens key:                HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler
  Opens key:                HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  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\wow6432node\microsoft\cryptography\offload
  Opens key:                HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}
  Opens key:                HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKLM\system\currentcontrolset\services\bfe
  Opens key:                HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}
  Opens key:                HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
  Opens key:                HKCU\software\classes\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
  Opens key:                HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
  Opens key:                HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}
  Opens key:                HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\treatas
  Opens key:                HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\progid
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid
  Opens key:                  HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                  HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                  HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\progid
  Opens key:                  HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler
  Opens key:                  HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler
  Opens key:                  HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}
  Opens key:                  HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
  Opens key:                  HKCU\software\classes\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
  Opens key:                  HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
  Opens key:                  HKLM\system\currentcontrolset\control\computername
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\treatas
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\treatas
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\progid
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid
  Opens key:                  HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
  Opens key:                  HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}
  Opens key:                  HKCU\software\classes\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\progid
  Opens key:                  HKCR\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}\progid
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler32
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler
  Opens key:                  HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprochandler
  Opens key:                  HKLM\software\wow6432node\microsoft\wbem\cimom
  Opens key:                  HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}
  Opens key:                  HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
  Opens key:                  HKCU\software\classes\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
  Opens key:                  HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}
  Opens key:                  HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\treatas
  Opens key:                  HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\progid
  Opens key:                  HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid
  Opens key:                  HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                  HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                  HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\progid
  Opens key:                  HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
  Opens key:                  HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
  Opens key:                  HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler32
  Opens key:                  HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
```

```
ce99a996d9ea}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler
  Opens key:                 HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}
  Opens key:                 HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-000000000001}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}
  Opens key:                 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\treatas
  Opens key:                 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\progid
  Opens key:                 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
  Opens key:                 HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:                 HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:                 HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\progid
  Opens key:                 HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\progid
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32
  Opens key:                 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler32
  Opens key:                 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler32
  Opens key:                 HKCU\software\classes\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler
  Opens key:                 HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler
  Opens key:                 HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}
  Opens key:                 HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32
  Opens key:                 HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}
  Opens key:                 HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
  Opens key:                 HKCU\software\classes\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32
  Opens key:                 HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32
  Opens key:                 HKLM\software\microsoft\windows defender
  Opens key:                 HKLM\system\currentcontrolset\services\netbt\linkage
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
  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:             HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:             HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:             HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:             HKCU\control panel\desktop[preferreduilanguages]
  Queries value:             HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[857bd61a8241ac81385ee957d8137887]
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:             HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:             HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:             HKCR\wow6432node\interface\{618736e0-3c3d-11cf-810c-
```

```
00aa00389b71}\proxystubclsid32[]
   Queries value:              HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
   Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   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:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[name]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parentfolder]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[description]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[relativepath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[parsingname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[infotip]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localizedname]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[icon]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[security]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresource]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[streamresourcetype]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[localredirectonly]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[roamable]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[precreate]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[stream]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[publishexpandedpath]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[attributes]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[foldertypeid]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{905e63b6-
c1bf-494e-b29c-65b732d3d21a}[initfolderhandler]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion[programfilesdir]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[category]
   Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-
a0fb-4bfc-874a-c0f2e0b9fa8e}[name]
   Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{7c5a40ef-a0fb-4bfc-874a-c0f2e0b9fa8e}[initfolderhandler]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
```

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

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
   Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
   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:            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\wow6432node\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\wow6432node\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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-
33be-4251-ba85-6007caedcf9d}[initfolderhandler]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-
6fba-4fcf-9d55-7b8e7f157091}[parentfolder]
```

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

```
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-980053277-1733835069-2361817685-1001[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\wow6432node\microsoft\windows\currentversion\internet settings\5.0\cache\cookies[peruseritem]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-908e-08a611b84ff6}[roamable]
  Queries value:
```

```
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-
c0e9-4171-908e-08a611b84ff6}[initfolderhandler]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  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\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[name]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
```

```
65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-
65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]
  Queries value:          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:          HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:          HKLM\software\microsoft\com3[com+enabled]
  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\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[category]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[name]
  Queries value:          HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\progid[]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[parentfolder]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[description]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[relativepath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[parsingname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[infotip]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[localizedname]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[icon]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[security]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[streamresource]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[streamresourcetype]
  Queries value:          HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:          HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[]
  Queries value:          HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[inprocserver32]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[localredirectonly]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[roamable]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[precreate]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[stream]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[publishexpandedpath]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[attributes]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
```

```
b784-432e-a781-5a1130a75963}[foldertypeid]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-
b784-432e-a781-5a1130a75963}[initfolderhandler]
  Queries value:              HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[]
  Queries value:              HKCR\wow6432node\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
  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:              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:              HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
```

```
settings[socketsendbufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[857bd61a8241ac81385ee957d8137887.exe]
  Queries value:              HKLM\software\wow6432node\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[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\wow6432node\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[enablehttptrace]
```

```
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[tcpautotuning]
  Queries value:            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\wow6432node\microsoft\windows\currentversion\internet
settings[disablebranchcache]
  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\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[searchlist]
  Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxysettingsperuser]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enabledhcp]
  Queries value:              HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpv6domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[dhcpnameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[dhcpnameserver]
  Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-
e1e01c1f69b5}[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-
806e6f6e6963}[enablemulticast]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:            HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:            HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:            HKLM\software\wow6432node\microsoft\tracing[enableconsoletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enablefiletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filetracingmask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enableconsoletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[consoletracingmask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filedirectory]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enablefiletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[filetracingmask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enableconsoletracing]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[consoletracingmask]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[maxfilesize]
  Queries value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[filedirectory]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:            HKLM\software\microsoft\sqmclient\windows\disabledprocesses[fbac773d]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[]
  Queries value:            HKCR\wow6432node\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[logging directory]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[logging]
  Queries value:            HKLM\software\wow6432node\microsoft\wbem\cimom[log file max size]
  Queries value:            HKCR\wow6432node\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic
provider[image path]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  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:              HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
   Queries value:              HKLM\software\microsoft\rpc\extensions[remoterpcdll]
   Queries value:              HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:              HKCR\wow6432node\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32[]
   Queries value:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]
   Queries value:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
   Queries value:              HKCR\wow6432node\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32[]
   Queries value:              HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-00c04fd8fdff}[]
   Queries value:              HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{674b6698-ee92-11d0-ad71-
00c04fd8fdff}\inprocserver32[threadingmodel]
   Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[processid]
   Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[enableprivateobjectheap]
   Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[contextlimit]
   Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[objectlimit]
   Queries value:              HKLM\software\wow6432node\microsoft\wbem\cimom[identifierlimit]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[en]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[en]
   Queries value:              HKCR\wow6432node\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32[]
   Queries value:              HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]
   Queries value:              HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
   Queries value:              HKCR\wow6432node\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32[]
   Queries value:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[]
   Queries value:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
   Queries value:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[]
   Queries value:              HKCR\wow6432node\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
   Queries value:              HKCR\wow6432node\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32[]
   Queries value:              HKCR\wow6432node\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32[]
   Queries value:              HKLM\software\microsoft\windows defender[disableantispyware]
   Queries value:              HKLM\system\currentcontrolset\services\netbt\linkage[export]
   Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enablefiletracing]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[enableconsoletracing]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filetracingmask]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[consoletracingmask]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[maxfilesize]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasapi32[filedirectory]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enablefiletracing]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[enableconsoletracing]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[filetracingmask]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[consoletracingmask]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[maxfilesize]
   Sets/Creates value:
HKLM\software\wow6432node\microsoft\tracing\857bd61a8241ac81385ee957d8137887_rasmancs[filedirectory]
```

```
  Value changes:            HKLM\software\microsoft\rpc[uuidsequencenumber]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
```