Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	404
Risk Level:	3
Date Processed:	2016-04-28 12:57:56 (UTC)
Processing Time:	61.68 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\00aca0729582792a46b971951043ff06.exe"
Sample ID:	101
Type:	basic
Owner:	admin
Label:	00aca0729582792a46b971951043ff06
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	203723 bytes
MD5:	00aca0729582792a46b971951043ff06
SHA256:	0afff2c277d7116b78d29818c8a9422daea4846a70a311c1696f262597209006
Description:	None

Pattern Matching Results

`1` HTTP connection - response code 404 (file not found) [HTTP, GET, POST, web, network, response code]

`3` Long sleep detected

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\windows\temp\00aca0729582792a46b971951043ff06.exe

["C:\windows\temp\00aca0729582792a46b971951043ff06.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
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\RasPbFile
Creates mutex:	\Sessions\1\BaseNamedObjects\IESQMMUTEX_0_208
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\!IETld!Mutex
Creates event:	\Security\LSA_AUTHENTICATION_INITIALIZED
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\BFE_Notify_Event_{ea4984cf-ef3a-4329-887f-12c7112c75a0}
Creates event:	\KernelObjects\MaximumCommitCondition

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Local
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Creates:	C:\Windows\Temp\HandWalletUpdate.original
Opens:	C:\Windows\Prefetch\00ACA0729582792A46B971951043F-1D996432.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\00aca0729582792a46b971951043ff06.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\System32\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\windows\temp\00aca0729582792a46b971951043ff06.ENU

```
Opens:                    C:\windows\temp\00aca0729582792a46b971951043ff06.ENU.DLL
Opens:                    C:\windows\temp\00aca0729582792a46b971951043ff06.EN
Opens:                    C:\windows\temp\00aca0729582792a46b971951043ff06.EN.DLL
Opens:                    C:\Windows\Temp
Opens:                    C:\Windows\Temp\00aca0729582792a46b971951043ff06.exe
Opens:                    C:\Windows\System32\uxtheme.dll
Opens:                    C:\windows\temp\dwmapi.dll
Opens:                    C:\Windows\System32\dwmapi.dll
Opens:                    C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:                    C:\windows\temp\HandWalletUpdate.original
Opens:                    C:http:\www.handwallet.com\update\
Opens:                    C:\Windows\System32\wininet.dll
Opens:                    C:\windows\temp\SspiCli.dll
Opens:                    C:\Windows\System32\sspicli.dll
Opens:                    C:\windows\temp\profapi.dll
Opens:                    C:\Windows\System32\profapi.dll
Opens:                    C:\Users\Admin
Opens:                    C:\Users\Admin\AppData\Local
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\desktop.ini
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\desktop.ini
Opens:                    C:\Users\Admin\AppData\Roaming
Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\History
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\History\desktop.ini
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
Opens:                    C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet
Files\Content.IE5\index.dat
Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
Opens:
C:\Users\Admin\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
Opens:                    C:\windows\temp\ntmarta.dll
Opens:                    C:\Windows\System32\ntmarta.dll
Opens:                    C:\windows\temp\dnsapi.DLL
Opens:                    C:\Windows\System32\dnsapi.dll
Opens:                    C:\windows\temp\iphlpapi.DLL
Opens:                    C:\Windows\System32\IPHLPAPI.DLL
Opens:                    C:\windows\temp\WINNSI.DLL
Opens:                    C:\Windows\System32\winnsi.dll
Opens:                    C:\windows\temp\RASAPI32.dll
Opens:                    C:\Windows\System32\rasapi32.dll
Opens:                    C:\windows\temp\rasman.dll
Opens:                    C:\Windows\System32\rasman.dll
Opens:                    C:\windows\temp\rtutils.dll
Opens:                    C:\Windows\System32\rtutils.dll
Opens:                    C:\ProgramData\Microsoft\Network\Connections\Pbk\
Opens:                    C:\Windows\System32\ras
Opens:                    C:\windows\temp\CRYPTBASE.dll
Opens:                    C:\Windows\System32\cryptbase.dll
Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Network\Connections\Pbk
Opens:                    C:\windows\temp\sensapi.dll
Opens:                    C:\Windows\System32\SensApi.dll
Opens:                    C:\Windows\System32\rpcss.dll
Opens:                    C:\Windows\System32\nlaapi.dll
Opens:                    C:\Windows\System32\NapiNSP.dll
Opens:                    C:\Windows\System32\pnrpnsp.dll
Opens:                    C:\Windows\System32\mswsock.dll
Opens:                    C:\Windows\System32\winrnr.dll
Opens:                    C:\Windows\System32\WSHTCPIP.DLL
Opens:                    C:\Windows\System32\wship6.dll
Opens:                    C:\windows\temp\dhcpcsvc6.DLL
Opens:                    C:\Windows\System32\dhcpcsvc6.dll
Opens:                    C:\windows\temp\dhcpcsvc.DLL
Opens:                    C:\Windows\System32\dhcpcsvc.dll
Opens:                    C:\windows\temp\rasadhlp.dll
Opens:                    C:\Windows\System32\rasadhlp.dll
Opens:                    C:\Windows\System32\drivers\etc\hosts
Opens:                    C:\Windows\System32\FWPUCLNT.DLL
Opens:                    C:\Windows\System32\netprofm.dll
Opens:                    C:\windows\temp\CRYPTSP.dll
Opens:                    C:\Windows\System32\cryptsp.dll
Opens:                    C:\Windows\System32\rsaenh.dll
Opens:                    C:\windows\temp\RpcRtRemote.dll
Opens:                    C:\Windows\System32\RpcRtRemote.dll
Opens:                    C:\Windows\System32\npmproxy.dll
Opens:                    C:\windows\temp\VERSION.dll
Opens:                    C:\Windows\System32\version.dll
```

Opens:	C:\Windows\System32\en-US\urlmon.dll.mui
Opens:	C:\Windows\Temp\HandWalletUpdate.original
Opens:	C:\windows\temp\HandWalletUpdate.info
Writes to:	C:\Windows\Temp\HandWalletUpdate.original
Reads from:	C:\Windows\Temp\00aca0729582792a46b971951043ff06.exe
Reads from:	C:\Windows\System32\drivers\etc\hosts
Reads from:	C:\Windows\Temp\HandWalletUpdate.original

Network Events

DNS query:	wpad
DNS query:	www.handwallet.com
DNS response:	handwallet.com ⇒ 198.71.157.117
Connects to:	198.71.157.117:80
Sends data to:	0.0.0.0:5355
Sends data to:	224.0.0.252:5355
Sends data to:	8.8.8.8:53
Sends data to:	handwallet.com:80 (198.71.157.117)
Receives data from:	8.8.8.8:53
Receives data from:	handwallet.com:80 (198.71.157.117)

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKLM\software\microsoft\tracing
Creates key:	HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32
Creates key:	HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\connections
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}\66-bc-c7-95-88-39
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings\wpad\66-bc-c7-95-88-39
Creates key:	HKCU\software\microsoft\windows nt\currentversion\network\location awareness
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[proxyserver]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[proxyoverride]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings[autoconfigurl]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKLM\software\microsoft\windows\currentversion\internet settings\zonemap[proxybypass]
Deletes value:	HKCU\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Deletes value:	HKLM\software\microsoft\windows\currentversion\internet settings\zonemap[intranetname]
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop\languageconfiguration
Opens key:	HKCU\control panel\desktop
Opens key:	HKCU\control panel\desktop\muicached
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument
Opens key:	HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:	HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:	HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKCU\software\borland\locales
Opens key:	HKLM\software\borland\locales

```
Opens key:              HKCU\software\borland\delphi\locales
Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:              HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:              HKCU\software\pantaray\qsetup\autoupdate
Opens key:              HKLM\system\currentcontrolset\services\crypt32
Opens key:              HKLM\software\microsoft\windows\currentversion\internet settings
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings
Opens key:              HKLM\software\policies
Opens key:              HKCU\software\policies
Opens key:              HKCU\software
Opens key:              HKLM\software
Opens key:              HKLM\software\policies\microsoft\internet explorer
Opens key:              HKLM\software\policies\microsoft\internet explorer\main
Opens key:              HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key:              HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key:              HKCU\software\microsoft\internet explorer\main\featurecontrol
Opens key:              HKLM\software\microsoft\internet explorer\main\featurecontrol
Opens key:              HKLM\software\microsoft\rpc
Opens key:              HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key:              HKLM\system\setup
Opens key:              HKLM\software\policies\microsoft\windows nt\rpc
Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
Opens key:              HKLM\software\microsoft\sqmclient\windows
Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}\propertybag
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key:              HKLM\software\policies\microsoft\windows\explorer
Opens key:              HKCU\software\policies\microsoft\windows\explorer
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}\propertybag
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
Opens key:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{2b0f765d-c0e9-4171-
908e-08a611b84ff6}\propertybag
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
a03a-e3ef65729f3d}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-
```

a03a-e3ef65729f3d}\propertybag
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
   Opens key: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}\propertybag
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
   Opens key: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
   Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
   Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_notify_unverified_spn_kb2385266
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_compat_use_connection_based_negotiate_auth_kb2151543
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
   Opens key: HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_exclude_invalid_client_cert_kb929477
   Opens key: HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545

```
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_utf8_for_basic_auth_kb967545
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_release_keys_on_unload_kb975619
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_security_flag_ignore_revocation_kb2275828
  Opens key:              HKLM\system\currentcontrolset\control\lsa\accessproviders
  Opens key:              HKLM\system\currentcontrolset\services\ldap
  Opens key:              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\1a6fc743
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32
```

```
    Opens key:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\profilelist
   Opens key:              HKLM\system\currentcontrolset\control\sqmservicelist
   Opens key:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
   Opens key:              HKLM\software\microsoft\sqmclient\windows\disabledsessions\
   Opens key:              HKU\
   Opens key:              HKCU\software\classes\
   Opens key:              HKCU\software\classes\autoproxytypes
   Opens key:              HKCR\autoproxytypes
   Opens key:              HKCU\software\classes\autoproxytypes\application/x-internet-signup
   Opens key:              HKCR\autoproxytypes\application/x-internet-signup
   Opens key:              HKCU\software\classes\autoproxytypes\application/x-ns-proxy-autoconfig
   Opens key:              HKCR\autoproxytypes\application/x-ns-proxy-autoconfig
   Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
   Opens key:              HKLM\system\currentcontrolset\services\dnscache\parameters
   Opens key:              HKLM\software\policies\microsoft\windows nt\dnsclient
   Opens key:              HKLM\system\currentcontrolset\services\dns
   Opens key:              HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
   Opens key:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens key:              HKLM\software\policies\microsoft\system\dnsclient
   Opens key:              HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:              HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
   Opens key:              HKLM\system\currentcontrolset\services\psched\parameters\winsock
   Opens key:              HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
   Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
   Opens key:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6
   Opens key:              HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
   Opens key:              HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
   Opens key:              HKLM\system\currentcontrolset\services\tcpip\linkage
   Opens key:              HKLM\software\microsoft\com3
   Opens key:              HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
   Opens key:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}
   Opens key:              HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\treatas
   Opens key:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\treatas
   Opens key:              HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\progid
   Opens key:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\progid
   Opens key:              HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32
   Opens key:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32
   Opens key:              HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler32
   Opens key:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprochandler32
   Opens key:              HKCU\software\classes\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprochandler
   Opens key:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprochandler
   Opens key:              HKLM\software\microsoft\rpc\extensions
   Opens key:              HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
   Opens key:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
   Opens key:              HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\treatas
   Opens key:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
   Opens key:              HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\progid
```

```
Opens key:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key:              HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprocserver32
Opens key:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
Opens key:              HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler32
Opens key:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32
Opens key:              HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-
001185ad2b89}\inprochandler
Opens key:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler
Opens key:              HKCU\software\classes\appid\00aca0729582792a46b971951043ff06.exe
Opens key:              HKCR\appid\00aca0729582792a46b971951043ff06.exe
Opens key:              HKLM\software\microsoft\ole\appcompat
Opens key:              HKLM\system\currentcontrolset\control\lsa
Opens key:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
Opens key:              HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key:              HKLM\software\policies\microsoft\cryptography
Opens key:              HKLM\software\microsoft\cryptography
Opens key:              HKLM\software\microsoft\cryptography\offload
Opens key:              HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
Opens key:              HKCR\interface\{00000134-0000-0000-c000-000000000046}
Opens key:              HKCU\software\classes\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32
Opens key:              HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key:              HKLM\system\currentcontrolset\services\bfe
Opens key:              HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
Opens key:              HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}
Opens key:              HKCU\software\classes\interface\{d0074ffd-570f-4a9b-8d69-
199fdba5723b}\proxystubclsid32
Opens key:              HKCR\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32
Opens key:              HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key:              HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\treatas
Opens key:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
Opens key:              HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\progid
Opens key:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key:              HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32
Opens key:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
Opens key:              HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler32
Opens key:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
Opens key:              HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprochandler
Opens key:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler
Opens key:              HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
Opens key:              HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}
Opens key:              HKCU\software\classes\interface\{26656eaa-54eb-4e6f-8f85-
4f0ef901a406}\proxystubclsid32
Opens key:              HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32
Opens key:              HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
Opens key:              HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}
Opens key:              HKCU\software\classes\interface\{8a40a45d-055c-4b62-abd7-
6d613e2ceaec}\proxystubclsid32
Opens key:              HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32
Opens key:              HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
Opens key:              HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}
Opens key:              HKCU\software\classes\interface\{55272a00-42cb-11ce-8135-
00aa004bb851}\proxystubclsid32
Opens key:              HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32
Opens key:              HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key:              HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
Opens key:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
Opens key:              HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\progid
Opens key:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key:              HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
Opens key:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
Opens key:              HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
Opens key:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
Opens key:              HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler
Opens key:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
Opens key:              HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
```

```
Opens key:              HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}
Opens key:              HKCU\software\classes\interface\{bcd1de7e-2db1-418b-b047-
4a74e101f8c1}\proxystubclsid32
Opens key:              HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32
Opens key:              HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
Opens key:              HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}
Opens key:              HKCU\software\classes\interface\{2a1c9eb2-df62-4154-b800-
63278fcb8037}\proxystubclsid32
Opens key:              HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}
Opens key:              HKLM\system\currentcontrolset\services\netbt\linkage
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_include_port_in_spn_kb908209
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\protocoldefaults\
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key:              HKLM\software\policies\microsoft\internet explorer\security
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones\
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
Opens key:              HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
Opens key:              HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
```

```
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
Opens key:              HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
Opens key:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
Opens key:              HKCU\software\microsoft\internet explorer\ietld
Opens key:              HKLM\system\currentcontrolset\control\cmf\config
Opens key:              HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key:              HKCU\software\microsoft\windows\currentversion\policies\explorer
Queries value:          HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value:          HKCU\control panel\desktop[preferreduilanguages]
Queries value:          HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value:          HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[00aca0729582792a46b971951043ff06]
Queries value:          HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value:          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value:          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value:          HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:          HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value:          HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value:          HKLM\software\microsoft\windows\currentversion\internet
```

settings[disableimprovedzonecheck]
   Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[security_hklm_only]
   Queries value: HKLM\system\currentcontrolset\control\wmi\security[0cfe0455-93ba-440d-
a3fe-553973d0b723]
   Queries value: HKLM\system\currentcontrolset\control\wmi\security[797fabac-7b58-4796-
b924-d51178a59ce4]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
   Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
   Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[secureprotocols]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
   Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
   Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
   Queries value: HKCU\software\policies\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
   Queries value: HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
   Queries value: HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
   Queries value: 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: HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
   Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
   Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
   Queries value: HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[category]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[name]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parentfolder]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[description]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[relativepath]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[parsingname]
   Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-

```
ba85-6007caedcf9d}[infotip]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localizedname]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[icon]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[security]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresource]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[streamresourcetype]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[localredirectonly]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[roamable]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[precreate]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[stream]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[publishexpandedpath]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[attributes]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[foldertypeid]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}[initfolderhandler]
     Queries value:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[category]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[name]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parentfolder]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[description]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[relativepath]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[parsingname]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[infotip]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localizedname]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[icon]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[security]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresource]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[streamresourcetype]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[localredirectonly]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
```

9d55-7b8e7f157091}[roamable]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[precreate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[stream]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[publishexpandedpath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[attributes]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[foldertypeid]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f1b32785-6fba-4fcf-
9d55-7b8e7f157091}[initfolderhandler]
    Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[category]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[name]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parentfolder]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[description]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[relativepath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[parsingname]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[infotip]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localizedname]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[icon]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[security]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresource]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[streamresourcetype]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[localredirectonly]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[roamable]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[precreate]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[stream]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[publishexpandedpath]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[attributes]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[foldertypeid]
    Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}[initfolderhandler]
    Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
2160590473-689474908-1361669368-1002[profileimagepath]

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

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

a781-5a1130a75963}[icon]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[security]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[streamresource]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[streamresourcetype]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[localredirectonly]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[roamable]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[precreate]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[stream]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[publishexpandedpath]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[attributes]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[foldertypeid]
     Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{d9dc8a3b-b784-432e-
a781-5a1130a75963}[initfolderhandler]
     Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
     Queries value: HKCU\software\microsoft\windows\currentversion\internet

```
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Queries value:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enableautoproxyresultcache]
  Queries value:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings[displayscriptdownloadfailureui]
  Queries value:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsservername]
  Queries value:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings[mbcsapiforcrack]
  Queries value:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings[utf8servernameres]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:               HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:               HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[00aca0729582792a46b971951043ff06.exe]
  Queries value:               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:               HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
```

```
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
   Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
   Queries value:              HKLM\software\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\system\currentcontrolset\control\lsa\accessproviders[martaextension]
   Queries value:              HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:              HKLM\system\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Queries value:              HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
   Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[tcpautotuning]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
```

```
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
     Queries value:
HKLM\system\currentcontrolset\services[winsock2\parameters\namespace_catalog5[serial_access_num]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
     Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
     Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
    Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
    Queries value:                HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadoverride]
    Queries value:                HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
    Queries value:                HKCU\software\microsoft\windows\currentversion\internet
settings[nonetautodial]
    Queries value:                HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
    Queries value:                HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
    Queries value:                HKLM\software\microsoft\windows\currentversion\internet
settings[disablebranchcache]
    Queries value:                HKLM\software\microsoft\tracing[enableconsoletracing]
    Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[enablefiletracing]
    Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[filetracingmask]
    Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[enableconsoletracing]
    Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[consoletracingmask]
    Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[maxfilesize]
    Queries value:
```

```
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[filedirectory]
   Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[enablefiletracing]
   Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[filetracingmask]
   Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[enableconsoletracing]
   Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[consoletracingmask]
   Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[maxfilesize]
   Queries value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[filedirectory]
   Queries value:               HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
   Queries value:               HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
   Queries value:               HKLM\software\microsoft\sqmclient\windows\disabledprocesses[5aa76484]
   Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
   Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
   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:               HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigcustomua]
   Queries value:               HKCR\autoproxytypes\application/x-internet-signup[dllfile]
   Queries value:               HKCR\autoproxytypes\application/x-internet-signup[fileextensions]
   Queries value:               HKCR\autoproxytypes\application/x-internet-signup[default]
   Queries value:               HKCR\autoproxytypes\application/x-internet-signup[flags]
   Queries value:               HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[dllfile]
   Queries value:               HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[fileextensions]
   Queries value:               HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[default]
   Queries value:               HKCR\autoproxytypes\application/x-ns-proxy-autoconfig[flags]
   Queries value:               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[00aca0729582792a46b971951043ff06.exe]
   Queries value:               HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable[*]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
```

```
     Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
     Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
     Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
     Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
     Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
     Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
```

```
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
    Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
    Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
    Queries value:              HKLM\system\currentcontrolset\services\winsock\parameters[transports]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
    Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
    Queries value:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
    Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
    Queries value:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
    Queries value:              HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip6[winsock 2.0 provider id]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[minsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[maxsockaddrlength]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[usedelayedacceptance]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[helperdllname]
    Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache[shutdownonidle]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[searchlist]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enabledhcp]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpdomain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpv6domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[nameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[dhcpnameserver]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enabledhcp]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationenabled]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registeradaptername]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[domain]
    Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpdomain]
```

```
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[nameserver]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[dhcpnameserver]
     Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[queryadaptername]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[disableadapterdomainname]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[registrationmaxaddresscount]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[maxnumberofaddressestoregister]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}[enablemulticast]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[queryadaptername]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disableadapterdomainname]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[disabledynamicupdate]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enableadapterdomainnameregistration]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[registrationmaxaddresscount]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[maxnumberofaddressestoregister]
     Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}[enablemulticast]
     Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
     Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
     Queries value:              HKLM\software\microsoft\com3[com+enabled]
     Queries value:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}[]
     Queries value:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[inprocserver32]
     Queries value:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-199fdba5723b}\inprocserver32[]
     Queries value:              HKCR\clsid\{dcb00c01-570f-4a9b-8d69-
199fdba5723b}\inprocserver32[threadingmodel]
     Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
     Queries value:              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
     Queries value:              HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
     Queries value:              HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
     Queries value:              HKLM\software\microsoft\ole[defaultaccesspermission]
     Queries value:              HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
     Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
     Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
     Queries value:              HKLM\system\currentcontrolset\control\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\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\interface\{d0074ffd-570f-4a9b-8d69-199fdba5723b}\proxystubclsid32[]
     Queries value:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
     Queries value:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
     Queries value:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
     Queries value:              HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
     Queries value:              HKCR\interface\{26656eaa-54eb-4e6f-8f85-4f0ef901a406}\proxystubclsid32[]
     Queries value:              HKCR\interface\{8a40a45d-055c-4b62-abd7-6d613e2ceaec}\proxystubclsid32[]
```

```
Queries value:              HKCR\interface\{55272a00-42cb-11ce-8135-00aa004bb851}\proxystubclsid32[]
Queries value:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
Queries value:              HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
Queries value:              HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
Queries value:              HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
Queries value:              HKCR\interface\{bcd1de7e-2db1-418b-b047-4a74e101f8c1}\proxystubclsid32[]
Queries value:              HKCR\interface\{2a1c9eb2-df62-4154-b800-63278fcb8037}\proxystubclsid32[]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[autoproxydetecttype]
Queries value:              HKLM\system\currentcontrolset\services\netbt\linkage[export]
Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[00aca0729582792a46b971951043ff06.exe]
Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_mime_handling[*]
Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[00aca0729582792a46b971951043ff06.exe]
Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck[*]
Queries value:              HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[00aca0729582792a46b971951043ff06.exe]
Queries value:              HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[00aca0729582792a46b971951043ff06.exe]
Queries value:              HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
Queries value:              HKLM\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value:              HKCU\software\policies\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietldversionlow]
Queries value:              HKCU\software\microsoft\internet explorer\ietld[ietldversionhigh]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[1a10]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[enablefiletracing]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[enableconsoletracing]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[filetracingmask]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[consoletracingmask]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[maxfilesize]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasapi32[filedirectory]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[enablefiletracing]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[enableconsoletracing]
Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[filetracingmask]
```

Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[consoletracingmask]
   Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[maxfilesize]
   Sets/Creates value:
HKLM\software\microsoft\tracing\00aca0729582792a46b971951043ff06_rasmancs[filedirectory]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpaddecisionreason]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpaddecisiontime]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpaddecision]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpadnetworkname]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\66-bc-c7-95-88-39[wpaddecisionreason]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\66-bc-c7-95-88-39[wpaddecisiontime]
   Sets/Creates value: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\66-bc-c7-95-88-39[wpaddecision]
   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\connections[defaultconnectionsettings]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad[wpadlastnetwork]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpaddecisionreason]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpaddecisiontime]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpaddecision]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\{74b1e0bf-aea3-4a90-8faf-011a15d24826}[wpadnetworkname]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\66-bc-c7-95-88-39[wpaddecisionreason]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\66-bc-c7-95-88-39[wpaddecisiontime]
   Value changes: HKCU\software\microsoft\windows\currentversion\internet
settings\wpad\66-bc-c7-95-88-39[wpaddecision]