

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 622, Task ID: 2434

Task ID:	2434
Risk Level:	8
Date Processed:	2016-02-22 05:29:43 (UTC)
Processing Time:	61.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe"
Sample ID:	622
Type:	basic
Owner:	admin
Label:	33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui
File Size:	54272 bytes
MD5:	75984f5cee7f9e64b9ffe44f60df8764
SHA256:	33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99
Description:	None

## Pattern Matching Results

- 3 HTTP connection - response code 200 (success) [HTTP, POST, GET, web, network, response code]
- 4 Reads process memory
- 6 Contacts service to find external IP address
- 8 Starts svchost.exe
- 7 Writes to memory of system processes

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe
["c:\windows\temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe" ]	
Creates process:	C:\WINDOWS\system32\svchost.exe [svchost.exe]
Loads service:	RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Reads from process:	PID: 244 C:\WINDOWS\system32\svchost.exe
Writes to process:	PID: 244 C:\WINDOWS\system32\svchost.exe
Terminates process:	C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

## Named Object Events

Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_Mutex
Creates mutex:	\BaseNamedObjects\c:\documents and settings\admin!local settings!temporary internet files!content.ie5!
Creates mutex:	\BaseNamedObjects\c:\documents and settings\admin!cookies!
Creates mutex:	\BaseNamedObjects\c:\documents and settings\admin!local settings!history!history.ie5!
Creates mutex:	\BaseNamedObjects\WininetConnectionMutex
Creates mutex:	\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex:	\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

## File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\QXMNBKF\icanhazip_com[1].txt
Opens:	C:\WINDOWS\Prefetch\33A18D17F6F150459E8EB2593A364-3910D469.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\COMCTL32.dll.124.Config
Opens:	C:\WINDOWS\system32\MSCTF.dll

```

Opens: C:\WINDOWS\system32\MSCTIME.IME
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\system32\svchost.exe
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\sysrest.sdb
Opens: C:\WINDOWS\system32
Opens: C:\
Opens: C:\WINDOWS
Opens: C:\WINDOWS\system32\svchost.exe.Manifest
Opens: C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
Opens: C:\WINDOWS\system32\shimeng.dll
Opens: C:\WINDOWS\AppPatch\AcGenral.dll
Opens: C:\WINDOWS\system32\winmm.dll
Opens: C:\WINDOWS\system32\msacm32.dll
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens: C:\WINDOWS\system32\urlmon.dll.123.Config
Opens: C:\WINDOWS\system32\wininet.dll.123.Manifest
Opens: C:\WINDOWS\system32\wininet.dll.123.Config
Opens:
C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe
Opens: C:\WINDOWS\Temp\5277c511-40ed-4b65-8746-20554de913a0
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\History
Opens: C:\Documents and Settings\Admin\Local Settings\History\History.IE5
Opens: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
Opens: C:\Documents and Settings\Admin\Cookies
Opens: C:\Documents and Settings\Admin\Cookies\index.dat
Opens: C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
Opens: C:\WINDOWS\system32\ws_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\rasapi32.dll
Opens: C:\WINDOWS\system32\rasman.dll
Opens: C:\WINDOWS\system32\netapi32.dll
Opens: C:\WINDOWS\system32\tapi32.dll
Opens: C:\WINDOWS\system32\rtutils.dll
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Manifest
Opens: C:\WINDOWS\system32\TAPI32.dll.124.Config
Opens: C:\AUTOEXEC.BAT
Opens: C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
Opens: C:\WINDOWS\system32\ras
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\Network\Connections\Pbk\
Opens: C:\WINDOWS\system32\sensapi.dll
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\rasadhlp.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\system32\drivers\etc\hosts
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\WINDOWS\system32\msv1_0.dll
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\WINDOWS\system32\msasn1.dll
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\Certificates
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CRLs
Opens: C:\Documents and Settings\Admin\Application
Data\Microsoft\SystemCertificates\My\CTLs
Opens: C:\WINDOWS\system32\wintrust.dll
Opens: C:\WINDOWS\system32\schannel.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMQBKF\icanhazip_com[1].txt
Reads from: C:\AUTOEXEC.BAT

```

Reads from: C:\WINDOWS\system32\drivers\etc\hosts  
Reads from: C:\WINDOWS\system32\rsaenh.dll  
Deletes:  
C:\WINDOWS\Temp\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe

## Network Events

DNS query:	icanhazip.com
DNS response:	icanhazip.com ⇒ 64.182.208.181
Connects to:	64.182.208.181:80
Connects to:	197.149.90.166:12232
Connects to:	173.216.247.74:443
Connects to:	77.48.30.156:443
Sends data to:	8.8.8.8:53
Sends data to:	icanhazip.com:80 (64.182.208.181)
Receives data from:	0.0.0.0:0
Receives data from:	icanhazip.com:80 (64.182.208.181)

## Windows Registry Events

Creates key:	HKCU\software\microsoft\multimedia\audio
Creates key:	HKCU\software\microsoft\multimedia\audio compression manager\
Creates key:	HKCU\software\microsoft\multimedia\audio compression manager\msacm
Creates key:	HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00	
Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders	
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKLM\software\microsoft\tracing
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders	
Creates key:	HKCU\software\microsoft\windows nt\currentversion\winlogon
Creates key:	HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:	HKCU\software\microsoft\windows\currentversion\internet
settings\connections	
Creates key:	HKCU\software\microsoft\windows nt\currentversion\network\location
awareness	
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
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]	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe	
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll	
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument
Opens key:	HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:	HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:	HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKCU\
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll	

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\msctf.dll  
Opens key:  
HKLM\software\microsoft\ctf\compatibility\33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99.exe  
Opens key: HKLM\software\microsoft\ctf\systemshared\  
Opens key: HKCU\keyboard layout\toggle  
Opens key: HKLM\software\microsoft\ctf\  
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\version.dll  
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\msctfime.ime  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\ole32.dll  
Opens key: HKLM\software\microsoft\ole  
Opens key: HKCR\interface  
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}  
Opens key: HKCU\software\microsoft\ctf  
Opens key: HKLM\software\microsoft\ctf\systemshared  
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls  
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\apphelp.dll  
Opens key: HKLM\system\wpa\tabletpc  
Opens key: HKLM\system\wpa\mediacenter  
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\svchost.exe  
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags  
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags  
Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects  
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}  
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes  
Opens key:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones  
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths  
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes  
Opens key:  
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones  
Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes  
 Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones  
 Opens key:

options\svchost.exe  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

options\acgenral.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shimeng.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\winmm.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\oleaut32.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msacm32.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shlwapi.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shell32.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\userenv.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\uxtheme.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm  
 Opens key: HKLM\software\microsoft\oleaut

Opens key: HKLM\software\microsoft\oleaut\userera

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm  
 Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm  
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610  
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723

Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1  
 Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet  
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2

Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm

Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance

Opens key: HKLM\system\setup

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack

Opens key: HKLM\system\currentcontrolset\control\productoptions

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders

Opens key: HKLM\software\policies\microsoft\windows\system

Opens key: HKCU\software\microsoft\windows\currentversion\thememanager

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\normaliz.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\iertutil.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\urlmon.dll

Opens key: HKCU\software\classes\  
 Opens key: HKCU\software\classes\protocols\name-space handler\  
 Opens key: HKCR\protocols\name-space handler  
 Opens key: HKCU\software\classes\protocols\name-space handler  
 Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet  
 settings  
 Opens key: HKLM\software\microsoft\windows\currentversion\internet settings  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet  
 settings  
 Opens key: HKCU\software\microsoft\internet  
 explorer\main\featurecontrol\feature\_protocol\_lockdown  
 Opens key: HKLM\software\microsoft\internet  
 explorer\main\featurecontrol\feature\_protocol\_lockdown  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet  
 settings\  
 Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol  
 Opens key: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol  
 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol  
 Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol  
 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: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\wininet.dll  
 Opens key: HKLM\system\currentcontrolset\control\wmi\security  
 Opens key: HKLM\system\currentcontrolset\control\computername  
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername  
 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\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: 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: 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\rpc\pagedbuffers  
 Opens key: HKLM\software\microsoft\rpc  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\svchost.exe\rpcthreadpoolthrottle  
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc  
 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\mshist012014033120140407  
 Opens key: HKCU\software\microsoft\windows\currentversion\internet  
 settings\5.0\cache\extensible cache\mshist012014041220140413  
 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\_use\_spn\_for\_ntlm\_auth\_disabled  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_use\_spn\_for\_ntlm\_auth\_disabled  
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\_passport\_check\_302\_for\_success\_kb949059  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_passport\_check\_302\_for\_success\_kb949059  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\ws2help.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\ws2\_32.dll  
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\00000004  
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\namespace\_catalog5  
Opens key:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000004  
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: 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: HKCU\software\microsoft\windows\currentversion\internet settings\http  
filters\rpa  
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings\http  
filters\rpa  
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\microsoft\windows nt\currentversion\image file execution  
options\netapi32.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\rasman.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\rtutils.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\tapi32.dll  
Opens key: HKLM\software\microsoft\windows\currentversion\telephony  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\rasapi32.dll  
Opens key: HKLM\software\microsoft\tracing\rasapi32  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist  
Opens key: HKLM\system\currentcontrolset\control\session manager\environment  
Opens key: HKLM\software\microsoft\windows\currentversion  
Opens key: HKU\  
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-  
1757981266-507921405-1957994488-1003  
Opens key: HKCU\environment  
Opens key: HKCU\volatile environment  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\sensapi.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\mswsock.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\rasadhlp.dll  
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: 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: 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\microsoft\windows\currentversion\internet  
settings\zonemap\domains\msn.com  
Opens key: HKLM\software\microsoft\windows\currentversion\internet  
settings\zonemap\domains\msn.com\related  
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\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\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: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient

```

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\iphlpapi.dll  
 Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage  
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\  
 Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces  
 Opens key: HKLM\system\currentcontrolset\services\netbt\parameters  
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7ceddc}  
 Opens key: HKLM\software\policies\microsoft\system\dnsclient  
 Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong  
 cryptographic provider  
 Opens key: HKLM\software\microsoft\rpc\securityservice  
 Opens key: HKLM\system\currentcontrolset\control\securityproviders  
 Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache  
 Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll  
 Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll  
 Opens key: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll  
 Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\msv1\_0.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\rsaenh.dll  
 Opens key: HKLM\software\policies\microsoft\cryptography  
 Opens key: HKLM\software\microsoft\cryptography  
 Opens key: HKLM\software\microsoft\cryptography\offload  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\hnetcfg.dll  
 Opens key: HKLM\system\currentcontrolset\services\winsock\parameters  
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\wshtcpip.dll  
 Opens key: HKCU\software\classes\mime\database\content type\text/plain;  
 charset=utf-8  
 Opens key: HKCR\mime\database\content type\text/plain; charset=utf-8  
 Opens key: HKCU\software\classes\mime\database\content type\text/plain  
 Opens key: HKCR\mime\database\content type\text/plain  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\msasn1.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\crypt32.dll  
 Opens key: HKLM\system\currentcontrolset\services\crypt32\performance  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1  
 Opens key: HKLM\software\microsoft\cryptography\oid  
 Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 0  
 Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype  
 0\certdllopenstoreprov  
 Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype  
 0\certdllopenstoreprov\#16  
 Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype  
 0\certdllopenstoreprov\ldap  
 Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype 1  
 Opens key: HKLM\software\microsoft\cryptography\oid\encodingtype  
 1\certdllopenstoreprov  
 Opens key: HKCU\software\microsoft\systemcertificates\my\physicalstores  
 Opens key: HKCU\software\microsoft\systemcertificates\my  
 Opens key: HKCU\software\microsoft\systemcertificates\my\  
 Opens key: HKCU\software\microsoft\systemcertificates\my\certificates  
 Opens key: HKCU\software\microsoft\systemcertificates\my\crls  
 Opens key: HKCU\software\microsoft\systemcertificates\my\ctls  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\imagehlp.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\wintrust.dll  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\schannel.dll  
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]  
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
 Queries value:  
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\compatibility32[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
 compatibility[33a18d17f6f150459e8eb2593a364b558768a1c85f4ee897aed2b83e30cefe99]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls]  
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]  
 Queries value: HKCU\control panel\desktop[multiuianguageid]  
 Queries value: HKCU\control panel\desktop[smoothscroll]  
 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]

Queries value: HKCU\keyboard layout\toggle[language hotkey]  
Queries value: HKCU\keyboard layout\toggle[hotkey]  
Queries value: HKCU\keyboard layout\toggle[layout hotkey]  
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[criticalsectiontimeout]  
Queries value: HKLM\software\microsoft\ole[rlwlockresourcetimeout]  
Queries value: HKCR\interface[interfacehelperperdisableall]  
Queries value: HKCR\interface[interfacehelperperdisableallforole32]  
Queries value: HKCR\interface[interfacehelperperdisabletypelib]  
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperperdisableall]  
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperperdisableallforole32]  
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager[safeprocesssearchmode]  
Queries value: HKLM\system\currentcontrolset\control\session  
manager\appcompatibility[disableappcompat]  
Queries value: HKLM\system\wpa\mediacenter[installed]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticcodeenabled]  
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[hashalg]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemsizes]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[saferflags]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemdata]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemsizes]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[saferflags]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsizes]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsizes]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-

b91490411bfc}[hashalg]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsize]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[cache]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\compatibility32[svchost]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
compatibility[svchost]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]  
Queries value:  
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]  
Queries value: HKCU\software\microsoft\multimedia\audio\systemformats]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.imaadpcm]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.msadpcm]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]  
Queries value: HKLM\software\microsoft\windows

nt\currentversion\drivers32[msacm.msg711]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.msgsm610]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.trspch]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.msg723]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.msaudio1]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\drivers32[msacm.sl\_anet]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl\_anet[cfiltertags]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]  
Queries value: HKCU\software\microsoft\multimedia\audio compression  
manager\msacm[nopcmconverter]  
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority  
v4.00[priority1]  
Queries value: HKLM\system\setup[systemsetupinprogress]  
Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\winlogon[userenvdebuglevel]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\winlogon[chkacdebuglevel]  
Queries value: HKLM\system\currentcontrolset\control\productoptions[producttype]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[personal]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[local settings]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\winlogon[rsopdebuglevel]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]  
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]  
Queries value: HKCU\control panel\desktop[lamebuttontext]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[disableimprovedzonecheck]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown[svchost.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_protocol\_lockdown[\*]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-ab78-1084642581fb]  
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]  
Queries value:  
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[fromcachetimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[secureprotocols]  
Queries value: HKLM\software\policies\microsoft\internet  
explorer\main[security\_hkln\_only]  
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: HKCU\software\microsoft\windows\currentversion\internet  
settings[enablehttp1\_1]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[proxyhttp1.1]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[enablenegotiate]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablebasicoverclearchannel]  
Queries value: HKCU\software\microsoft\internet  
explorer\main\featurecontrol[feature\_clientauthcertfilter]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol[feature\_clientauthcertfilter]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[clientauthbuiltinui]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[syncmode5]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings\5.0\cache[sessionstarttimedefaultdeltasecs]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache[signature]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[peruseritem]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\content[peruseritem]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[cache]  
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: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[cookies]  
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]

[illegible]

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\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[svchost.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[disablent4rascheck]  
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[bypassftptimecheck]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[releasesocketduringauth]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[releasesocketduring401auth]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[releasesocketduring401auth]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet



settings[wpadsearchalldomains]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablelegacypreauthserver]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[disablelegacypreauthserver]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[bypasshttptnocachecheck]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[bypasshttptnocachecheck]  
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[dnscheenabled]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[dnscheentries]  
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[warnonbadcertsending]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[warnonbadcertrecv]  
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\services\winsock2\parameters\winsock\_registry\_version]  
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\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[storiesserviceclassinfo]  
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[storiesserviceclassinfo]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[librarypath]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[displaystring]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[enabled]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version]  
Queries value:  
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storiesserviceclassinfo]  
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[globaluseroffline]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[enableautodial]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[urlencoding]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[truncatefilename]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[badproxyexpiretime]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[svchost.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[\*]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]  
Queries value: HKLM\software\microsoft\tracing[enableconsoletracing]  
Queries value: HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]  
Queries value: HKLM\software\microsoft\tracing\rasapi32[filetracingmask]  
Queries value: HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]  
Queries value: HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]  
Queries value: HKLM\software\microsoft\tracing\rasapi32[maxfilesize]  
Queries value: HKLM\software\microsoft\tracing\rasapi32[filedirectory]  
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell  
folders[common appdata]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\profilelist[profilesdirectory]

Queries value: HKLM\software\microsoft\windows  
nt\currentversion\profilelist[allusersprofile]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\profilelist[defaultuserprofile]  
Queries value: HKLM\software\microsoft\windows\currentversion[programfilesdir]  
Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-  
1757981266-507921405-1957994488-1003[profileimagepath]  
Queries value: HKCU\software\microsoft\windows  
nt\currentversion\winlogon[parseautoexec]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[appdata]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[migrateproxy]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[proxyenable]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[proxyserver]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[proxyoverride]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[autoconfigurl]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\connections[savedlegacysettings]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\connections[defaultconnectionsettings]  
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]  
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]  
Queries value: HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]  
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[svchost.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[svchost.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[createuricachesize]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[createuricachesize]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[enablepunycode]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[enablepunycode]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zonemap[autodetect]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\3[1a10]  
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[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[filterclusterip]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]  
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]  
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[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[maxnumberofaddressesstoregister]  
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[updatezoneexcludefile]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatetopleveldomainzones]  
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]  
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[multicastlistenlevel]  
Queries value:  
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendlevel]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]  
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[queryadaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registeradaptername]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationmaxaddresscount]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxnumberofaddresstoregister]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]  
Queries value:  
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsbtlookuporder]  
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\software\microsoft\rpc\securityservice[10]  
Queries value:  
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]  
Queries value: HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]  
Queries value:  
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]  
Queries value: HKLM\software\microsoft\cryptography[machineguid]  
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]  
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]  
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]  
Queries value:  
HKLM\system\currentcontrolset\services\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: HKCR\mime\database\content type\text/plain[extension]  
Value changes: HKLM\software\microsoft\cryptography\rng[seed]  
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[cache]  
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[cookies]  
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[history]  
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell  
folders[common appdata]  
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[appdata]  
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\zonemap[proxybypass]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet  
settings\zonemap[intranetname]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet  
settings\zonemap[uncasintranet]  
Value changes: HKCU\software\microsoft\windows\currentversion\internet  
settings\zonemap[autodetect]