

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 101, Task ID: 403

Task ID:	403
Risk Level:	1
Date Processed:	2016-04-28 12:57:52 (UTC)
Processing Time:	61.39 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\00aca0729582792a46b971951043ff06.exe"
Sample ID:	101
Type:	basic
Owner:	admin
Label:	00aca0729582792a46b971951043ff06
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	203723 bytes
MD5:	00aca0729582792a46b971951043ff06
SHA256:	0afff2c277d7116b78d29818c8a9422daea4846a70a311c1696f262597209006
Description:	None

## Pattern Matching Results

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

## Static Events

Anomaly:	PE: Contains a virtual section
----------	--------------------------------

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\00aca0729582792a46b971951043ff06.exe
["c:\windows\temp\00aca0729582792a46b971951043ff06.exe" ]	
Loads service:	RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]

## 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	MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
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:\WINDOWS\Temp\HandWalletUpdate.original
Opens:	C:\WINDOWS\Prefetch\00ACA0729582792A46B971951043F-2EDA1F17.pf
Opens:	C:\Documents and Settings\Admin
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\Temp\00aca0729582792a46b971951043ff06.exe
Opens:	C:\WINDOWS\system32\imm32.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\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\Temp
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME

Opens:	C:\WINDOWS\system32\uxtheme.dll
Opens:	C:\windows\temp\HandWalletUpdate.original
Opens:	C:http://www.handwallet.com/update\
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:\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\ws2_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\winmm.dll
Opens:	C:\WINDOWS\system32\TAPI32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\TAPI32.dll.124.Config
Opens:	C:\AUTOEXEC.BAT
Opens:	C:\
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\msv1_0.dll
Opens:	C:\WINDOWS\system32\iphlpapi.dll
Opens:	C:\WINDOWS\system32\mswsock.dll
Opens:	C:\WINDOWS\system32\rasadhlp.dll
Opens:	C:\WINDOWS\system32\dnsapi.dll
Opens:	C:\WINDOWS\system32\drivers\etc\hosts
Opens:	C:\WINDOWS\system32\rsaenh.dll
Opens:	C:\WINDOWS\system32\crypt32.dll
Opens:	C:\WINDOWS\system32\hnetcfg.dll
Opens:	C:\WINDOWS\system32\wshtcpip.dll
Opens:	C:\WINDOWS\Temp\HandWalletUpdate.original
Opens:	C:\windows\temp\HandWalletUpdate.info
Writes to:	C:\WINDOWS\Temp\HandWalletUpdate.original
Reads from:	C:\WINDOWS\Temp\00aca0729582792a46b971951043ff06.exe
Reads from:	C:\AUTOEXEC.BAT
Reads from:	C:\WINDOWS\system32\drivers\etc\hosts
Reads from:	C:\WINDOWS\system32\rsaenh.dll
Reads from:	C:\WINDOWS\Temp\HandWalletUpdate.original

## Network Events

DNS query:	www.handwallet.com
DNS response:	handwallet.com ⇒ 198.71.157.117
Connects to:	198.71.157.117:80
Sends data to:	8.8.8.8:53
Sends data to:	handwallet.com:80 (198.71.157.117)
Receives data from:	0.0.0.0:0
Receives data from:	handwallet.com:80 (198.71.157.117)

## Windows Registry Events

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\00aca0729582792a46b971951043ff06.exe
  Opens key: HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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\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\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\msvcrt.dll
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.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\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\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: HKLM\software\microsoft\ole
  Opens key: HKCR\interface
  Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key: HKLM\software\microsoft\oleaut
  Opens key: HKLM\software\microsoft\oleaut\userera
  Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key: HKLM\system\setup
  Opens key: HKCU\
  Opens key: HKCU\software\policies\microsoft\control panel\desktop
  Opens key: HKCU\control panel\desktop
  Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key: HKCU\software\borland\locales
  Opens key: HKLM\software\borland\locales
  Opens key: HKCU\software\borland\delphi\locales
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\00aca0729582792a46b971951043ff06.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: HKCU\software\microsoft\ctf
  Opens key: HKLM\software\microsoft\ctf\systemshared
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key: HKCU\software\pantarray\qsetup\autoupdate

```

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: 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\00aca0729582792a46b971951043ff06.exe\rpc\threadpool\throttle  
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc  
 Opens key: HKLM\system\currentcontrolset\control\computername  
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername  
 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: 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\winmm.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\drivers32  
Opens key:  
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm  
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\image file execution  
options\userenv.dll  
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: 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\rpc\securityservice  
Opens key: HKLM\system\currentcontrolset\control\securityproviders  
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicashe  
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicashe\msapsspc.dll  
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicashe\digest.dll  
Opens key: HKLM\system\currentcontrolset\control\lsa\sspicashe\msnsspc.dll  
Opens key: HKLM\system\currentcontrolset\control\securityproviders\saslprofiles  
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\software\microsoft\windows nt\currentversion\image file execution  
options\msv1\_0.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\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\mswsock.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\rasadhlp.dll  
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\dnsclient\parameters  
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient  
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters  
Opens key:  
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}  
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\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  
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\compatibility32[00aca0729582792a46b971951043ff06]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
compatibility[00aca0729582792a46b971951043ff06]  
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: HKLM\system\currentcontrolset\control\session  
manager[criticalsectiontimeout]  
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]  
Queries value: HKCR\interface[interfacehelperdisableall]  
Queries value: HKCR\interface[interfacehelperdisableallforole32]  
Queries value: HKCR\interface[interfacehelperdisablealltypelib]  
Queries value: HKCR\interface\{00020400-0000-0000-c000-  
000000000046}[interfacehelperdisableall]  
Queries value: HKCR\interface\{00020400-0000-0000-c000-  
000000000046}[interfacehelperdisableallforole32]  
Queries value: HKLM\system\setup[systemsetupinprogress]  
Queries value: HKCU\control panel\desktop[multiuilanguageid]  
Queries value: HKCU\control panel\desktop[smoothscroll]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]  
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: HKCU\software\microsoft\ctf[disable thread input manager]  
 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[00aca0729582792a46b971951043ff06.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: 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\_hklm\_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[disablebasiccoverclearchannel]  
 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]  
 Queries value: HKCU\software\microsoft\windows\currentversion\internet  
 settings\5.0\cache\history[peruseritem]  
 Queries value: HKLM\software\microsoft\windows\currentversion\internet  
 settings\5.0\cache\history[peruseritem]  
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
 folders[history]  
 Queries value: HKCU\software\microsoft\windows\currentversion\internet  
 settings\5.0\cache\history[cacheprefix]  
 Queries value: HKCU\software\microsoft\windows\currentversion\internet  
 settings\5.0\cache\history[cachelimit]  
 Queries value: HKLM\software\microsoft\rpc[maxrpcsize]  
 Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

[illegible]

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[disablentlmprauth]  
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[00aca0729582792a46b971951043ff06.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_disable\_unicode\_handle\_closing\_callback[\*]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablecachingofsslpages]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[perusercookies]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[leashlegacycookies]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[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[disablelegacyprauthserver]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[disablelegacyprauthserver]  
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[bypasssslnocheck]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[enablehttptrace]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[nocheckautodialoverride]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[dontusednsloadbalancing]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[sharecredswithwinhttp]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[mimeexclusionlistforcache]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[headerexclusionlistforcache]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheenabled]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscacheentries]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[dnscachetimeout]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonpost]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnalwaysonpost]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonzonecrossing]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertsending]

Queries value: HKCU\software\microsoft\windows\currentversion\internet settings[warnonbadcertrevoking]

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]

[illegible]

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:  
 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\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: 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\software\microsoft\rpc\securityservice[10]  
 Queries value:  
 HKLM\system\currentcontrolset\control\securityproviders[securityproviders]  
 Queries value: HKLM\system\currentcontrolset\control\session  
 manager[safeprocesssearchmode]  
 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\internet  
explorer\main\featurecontrol\feature\_mime\_handling[00aca0729582792a46b971951043ff06.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_mime\_handling[\*]  
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[00aca0729582792a46b971951043ff06.exe]  
Queries value: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[00aca0729582792a46b971951043ff06.exe]  
Queries value: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_localmachine\_lockdown[\*]  
Queries value: 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[maxnumberofaddresstoregister]  
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}[registeradapternam]
  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}[maxnumberofaddressesstoregister]
  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\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]
  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]

```