

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 3326, Task ID: 812

Task ID:	812
Risk Level:	10
Date Processed:	2016-05-18 10:41:03 (UTC)
Processing Time:	9.0 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe"
Sample ID:	3326
Type:	basic
Owner:	admin
Label:	6f21fb21650da014d87426fa0bd8e7f2
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	177664 bytes
MD5:	6f21fb21650da014d87426fa0bd8e7f2
SHA256:	34f1a3cc2318939b243bfc434f9ecfa721574ded9a3958a970d0b817d536885f
Description:	None

## Pattern Matching Results

- 6 Checks task list from command line
- 10 Creates malicious events: Beebone [Trojan]
- 3 Long sleep detected
- 4 Terminates process under Windows subfolder

## Static Events

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

## Process/Thread Events

Creates process:	C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe
["c:\windows\temp\6f21fb21650da014d87426fa0bd8e7f2.exe" ]	
Creates process:	C:\WINDOWS\system32\cmd.exe ["C:\WINDOWS\system32\cmd.exe" /c tasklist&&del 6f21fb21650da014d87426fa0bd8e7f2.exe]
Creates process:	C:\WINDOWS\system32\tasklist.exe [tasklist]
Loads service:	RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Terminates process:	C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe
Terminates process:	C:\WINDOWS\system32\tasklist.exe
Terminates process:	C:\WINDOWS\system32\cmd.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\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 mutex:	\BaseNamedObjects\SHIMLIB_LOG_MUTEX
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\C:?WINDOWS?TEMP?6F21FB21650DA014D87426FA0BD8E7F2.EXE
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

## File System Events

Opens:	C:\WINDOWS\Prefetch\6F21FB21650DA014D87426FA0BD8E-130ADCA8.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\winmm.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\msvbvm60.dll

Opens: C:\WINDOWS\system32\rpcss.dll  
Opens: C:\WINDOWS\system32\MSCTF.dll  
Opens: C:\WINDOWS\system32\sxs.dll  
Opens: C:\WINDOWS\system32\MSCTFIME.IME  
Opens: C:\WINDOWS\system32\clbcatq.dll  
Opens: C:\WINDOWS\system32\comres.dll  
Opens: C:\WINDOWS\Registration\R0000000000007.clb  
Opens: C:\WINDOWS\Fonts\sserife.fon  
Opens: C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.exe  
Opens: C:\  
Opens: C:\WINDOWS\system32\urlmon.dll.123.Manifest  
Opens: C:\WINDOWS\system32\urlmon.dll.123.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\WindowsShell1.Manifest  
Opens: C:\WINDOWS\WindowsShell1.Config  
Opens: C:\WINDOWS\system32\wininet.dll.123.Manifest  
Opens: C:\WINDOWS\system32\wininet.dll.123.Config  
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\system32\comctl32.dll  
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest  
Opens: C:\WINDOWS\system32\comctl32.dll.124.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\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\ieframe.dll  
Opens: C:\Program Files\Internet Explorer\iexplore.exe  
Opens: C:\WINDOWS\system32\ieframe.dll.123.Manifest  
Opens: C:\WINDOWS\system32\ieframe.dll.123.Config  
Opens: C:\WINDOWS\system32\en-US\ieframe.dll.mui  
Opens: C:\WINDOWS\system32  
Opens: C:\WINDOWS  
Opens: C:\WINDOWS\system32\setupapi.dll  
Opens: C:\WINDOWS\system32\cmd.exe  
Opens: C:\WINDOWS\AppPatch\sysmain.sdb  
Opens: C:\WINDOWS\AppPatch\sysrest.sdb  
Opens: C:\WINDOWS\system32\cmd.exe.Manifest  
Opens: C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf  
Opens: C:  
Opens: C:\WINDOWS\AppPatch  
Opens: C:\WINDOWS\system32\wbem  
Opens: C:\WINDOWS\WinSxS  
Opens: C:\WINDOWS\system32\ntdll.dll  
Opens: C:\WINDOWS\system32\kernel32.dll  
Opens: C:\WINDOWS\system32\unicode.nls

Opens:	C:\WINDOWS\system32\locale.nls
Opens:	C:\WINDOWS\system32\sorttbls.nls
Opens:	C:\WINDOWS\system32\msvcrt.dll
Opens:	C:\WINDOWS\system32\user32.dll
Opens:	C:\WINDOWS\system32\gdi32.dll
Opens:	C:\WINDOWS\system32\shimeng.dll
Opens:	C:\WINDOWS\AppPatch\AcGenral.dll
Opens:	C:\WINDOWS\system32\advapi32.dll
Opens:	C:\WINDOWS\system32\rpcrt4.dll
Opens:	C:\WINDOWS\system32\secur32.dll
Opens:	C:\WINDOWS\system32\ole32.dll
Opens:	C:\WINDOWS\system32\oleaut32.dll
Opens:	C:\WINDOWS\system32\msacm32.dll
Opens:	C:\WINDOWS\system32\version.dll
Opens:	C:\WINDOWS\system32\shlwapi.dll
Opens:	C:\WINDOWS\system32\userenv.dll
Opens:	C:\WINDOWS\system32\uxtheme.dll
Opens:	C:\WINDOWS\system32\ctype.nls
Opens:	C:\WINDOWS\system32\sortkey.nls
Opens:	C:\WINDOWS\system32\apphelp.dll
Opens:	C:\WINDOWS\system32\wbem\wmic.exe
Opens:	C:\WINDOWS\WINHELP.INI
Opens:	C:\Documents and Settings
Opens:	C:\WINDOWS\system32\tasklist.exe
Opens:	C:\WINDOWS\system32\tasklist.exe.Manifest
Opens:	C:\WINDOWS\Prefetch\TASKLIST.EXE-10D94B23.pf
Opens:	C:\WINDOWS\system32\wbem\framedyn.dll
Opens:	C:\WINDOWS\system32\dbghelp.dll
Opens:	C:\WINDOWS\system32\winlogon.exe
Opens:	C:\WINDOWS\system32\xpssp2res.dll
Opens:	C:\WINDOWS\system32\wbem\wbemprox.dll
Opens:	C:\WINDOWS\system32\wbem\wbemcomn.dll
Opens:	C:\WINDOWS\system32\winsta.dll
Opens:	C:\WINDOWS\system32\wbem\wbemsvc.dll
Opens:	C:\WINDOWS\system32\wbem\fastprox.dll
Opens:	C:\WINDOWS\system32\msvcp60.dll
Opens:	C:\WINDOWS\system32\ntdsapi.dll
Reads from:	C:\WINDOWS\Registration\R0000000000007.clb
Reads from:	C:\WINDOWS\Temp\6f21fb21650da014d87426fa0bd8e7f2.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\system32\cmd.exe
Reads from:	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

## Network Events

DNS query:	80170.z0dns.com
Sends data to:	8.8.8.8:53
Receives data from:	0.0.0.0:0

## 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
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0000000000008352
Creates key:	HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key:	HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
Creates key:	HKLM\software\microsoft\windows\currentversion\shell extensions\cached
Creates key:	HKCU\software\microsoft\windows\currentversion\shell extensions\cached
Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
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:	HKLM\software\microsoft\wbem\cimom
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\6f21fb21650da014d87426fa0bd8e7f2.exe
  Opens key: HKLM\system\currentcontrolset\control\terminal server
  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\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\winlogon
  Opens key: HKLM\
  Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
  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\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\image file execution
options\gdi32.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\imm32.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\ole
  Opens key: HKCR\interface
  Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key: HKLM\software\microsoft\oleaut
  Opens key: HKLM\software\microsoft\oleaut\userera
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvbvm60.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: 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\msctf.dll
  Opens key: HKLM\software\microsoft\ctf\compatibility\6f21fb21650da014d87426fa0bd8e7f2.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\image file execution
options\sxs.dll
  Opens key: HKLM\system\setup
  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\system\currentcontrolset\control\locale\codepage
  Opens key: HKLM\software\microsoft\vba\monitors
  Opens key: HKLM\software\microsoft\com3
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cibcatq.dll

```

Opens key: HKLM\software\microsoft\com3\debug  
 Opens key: HKCU\software\classes\  
 Opens key: HKLM\software\classes  
 Opens key: HKU\  
 Opens key: HKCR\clsid  
 Opens key: HKCU\software\classes\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}  
 Opens key: HKCR\clsid\{85847f48-d652-4fd3-9cd1-3ddafdba1a15}  
 Opens key: HKCU\software\classes\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}  
 Opens key: HKCR\clsid\{a450fe5b-6ab7-4a3c-9cf3-3cee05d360c1}  
 Opens key: HKCU\software\classes\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}  
 Opens key: HKCR\clsid\{56d37229-f433-4eef-a6a7-b69dd0e003a3}  
 Opens key: HKCU\software\classes\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}  
 Opens key: HKCR\clsid\{074c6e97-3f4e-4659-9428-62a3d81a47c1}  
 Opens key: HKCU\software\classes\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb}  
 Opens key: HKCR\clsid\{98e514e2-7646-40b7-9b56-9292aacf45cb}  
 Opens key: HKCU\software\classes\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b}  
 Opens key: HKCR\clsid\{1ec267b1-9ab3-4fd2-840e-ec868c13387b}  
 Opens key: HKCU\software\classes\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54}  
 Opens key: HKCR\clsid\{f3aaac74-c3f9-4f8e-a603-5e1ca200bf54}  
 Opens key: HKLM\system\currentcontrolset\services\disk\enum  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\shlwapi.dll  
 Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance  
 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: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\comctl32.dll  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\wininet.dll  
 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\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: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\shell32.dll  
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\6f21fb21650da014d87426fa0bd8e7f2.exe\rpcthreadpoolthrottle  
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: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature\_http\_username\_password\_disable  
Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature\_http\_username\_password\_disable  
Opens key: HKLM\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\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: 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: 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\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-
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\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: HKLM\system\currentcontrolset\services\netbt\linkage
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\6f21fb21650da014d87426fa0bd8e7f2.exe
  Opens key: HKCU\software\microsoft\windows\currentversion\explorer
  Opens key: HKLM\software\microsoft\windows\currentversion\explorer
  Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace

```

Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-e366-4d22-bc06-4ada335c892b}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{1f4de370-d627-11d1-ba4f-00a0c91eedba}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-ad25-11d0-98a8-0800361b1103}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-5081-101b-9f08-00aa002f954e}  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\0000000000008352\desktop\namespace  
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder  
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder  
Opens key: HKCU\software\classes\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder  
Opens key: HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder  
Opens key:  
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{871c5380-42a0-1069-a2ea-08002b30309d}  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll  
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\treatas  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver32  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver  
Opens key: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\localserver  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ieframe.dll  
Opens key: HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe  
Opens key: HKLM\software\microsoft\internet explorer\setup  
Opens key: HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib  
Opens key: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib  
Opens key: HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}  
Opens key: HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}  
Opens key: HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32  
Opens key: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32  
Opens key: HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32  
Opens key: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32  
Opens key: HKCU\software\classes\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder  
Opens key: HKCR\clsid\{11016101-e366-4d22-bc06-4ada335c892b}\shellfolder  
Opens key: HKCU\software\classes\clsid\{1f4de370-d627-11d1-ba4f-

00a0c91eedba}\shellfolder  
Opens key: HKCR\clsid\{1f4de370-d627-11d1-ba4f-00a0c91eedba}\shellfolder  
Opens key: HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder  
0800361b1103}\shellfolder  
Opens key: HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder  
Opens key: HKCU\software\classes\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder  
00aa002f954e}\shellfolder  
Opens key: HKCR\clsid\{645ff040-5081-101b-9f08-00aa002f954e}\shellfolder  
Opens key: HKCU\software\classes\clsid\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}\shellfolder  
00a0c90dc849}\shellfolder  
Opens key: HKCR\clsid\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}\shellfolder  
Opens key:  
HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks  
Opens key: HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32  
00c04fd91972}\inprocserver32  
Opens key: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32  
Opens key: HKLM\software\microsoft\windows\currentversion\app\_paths\cmd.exe  
Opens key: HKLM\software\microsoft\windows\currentversion\policies\associations  
Opens key: HKCU\software\microsoft\windows\currentversion\policies\associations  
Opens key: HKCU\software\classes\ .exe  
Opens key: HKCR\ .exe  
Opens key: HKCU\software\classes\ .ade  
Opens key: HKCR\ .ade  
Opens key: HKCU\software\classes\ .adp  
Opens key: HKCR\ .adp  
Opens key: HKCU\software\classes\ .app  
Opens key: HKCR\ .app  
Opens key: HKCU\software\classes\ .asp  
Opens key: HKCR\ .asp  
Opens key: HKCU\software\classes\ .bas  
Opens key: HKCR\ .bas  
Opens key: HKCU\software\classes\ .bat  
Opens key: HKCR\ .bat  
Opens key: HKCU\software\classes\ .cer  
Opens key: HKCR\ .cer  
Opens key: HKCU\software\classes\ .chm  
Opens key: HKCR\ .chm  
Opens key: HKCU\software\classes\ .cmd  
Opens key: HKCR\ .cmd  
Opens key: HKCU\software\classes\ .com  
Opens key: HKCR\ .com  
Opens key: HKCU\software\classes\ .cpl  
Opens key: HKCR\ .cpl  
Opens key: HKCU\software\classes\ .crt  
Opens key: HKCR\ .crt  
Opens key: HKCU\software\classes\ .csh  
Opens key: HKCR\ .csh  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas  
00c04fb6bfc4}\treatas  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32  
00c04fb6bfc4}\inprocserver32  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86  
00c04fb6bfc4}\inprocserverx86  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32  
00c04fb6bfc4}\localserver32  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32  
00c04fb6bfc4}\inprochandler32  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86  
00c04fb6bfc4}\inprochandlerx86  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver  
00c04fb6bfc4}\localserver  
Opens key: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_initialize\_urlaction\_shellexecute\_to\_allow\_kb936610  
Opens key: HKCU\software\microsoft\internet  
explorer\main\featurecontrol\feature\_zones\_default\_drive\_intranet\_kb941000  
Opens key: HKLM\software\microsoft\internet  
explorer\main\featurecontrol\feature\_zones\_default\_drive\_intranet\_kb941000  
Opens key:  
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-a2d8-08002b30309d}  
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32

Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\setupapi.dll  
 Opens key: HKLM\system\currentcontrolset\control\minint  
 Opens key: HKLM\system\wpa\pnp  
 Opens key: HKLM\software\microsoft\windows\currentversion\setup  
 Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels  
 Opens key:  
 HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume  
 Opens key:  
 HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\  
 Opens key: HKCU\software\classes\drive\shellex\folderextensions  
 Opens key: HKCR\drive\shellex\folderextensions  
 Opens key: HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}  
 Opens key: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}  
 Opens key: HKCU\software\classes\directory  
 Opens key: HKCR\directory  
 Opens key: HKCU\software\classes\directory\curver  
 Opens key: HKCR\directory\curver  
 Opens key: HKCR\directory\  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\system  
 Opens key: HKCU\software\classes\directory\shellex\iconhandler  
 Opens key: HKCR\directory\shellex\iconhandler  
 Opens key: HKCU\software\classes\directory\clsid  
 Opens key: HKCR\directory\clsid  
 Opens key: HKCU\software\classes\folder  
 Opens key: HKCR\folder  
 Opens key: HKCU\software\classes\folder\clsid  
 Opens key: HKCR\folder\clsid  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\fileexts\exe  
 Opens key: HKCU\software\classes\exefile  
 Opens key: HKCR\exefile  
 Opens key: HKCU\software\classes\exefile\curver  
 Opens key: HKCR\exefile\curver  
 Opens key: HKCR\exefile\  
 Opens key: HKCU\software\classes\exefile\shellex\iconhandler  
 Opens key: HKCR\exefile\shellex\iconhandler  
 Opens key: HKCU\software\classes\systemfileassociations\exe  
 Opens key: HKCR\systemfileassociations\exe  
 Opens key: HKCU\software\classes\systemfileassociations\application  
 Opens key: HKCR\systemfileassociations\application  
 Opens key: HKCU\software\classes\exefile\clsid  
 Opens key: HKCR\exefile\clsid  
 Opens key: HKCU\software\classes\  
 Opens key: HKCR\  
 Opens key: HKCU\software\classes\\*\clsid  
 Opens key: HKCR\\*\clsid  
 Opens key: HKCU\software\classes\exefile\shell  
 Opens key: HKCR\exefile\shell  
 Opens key: HKCU\software\classes\exefile\shell\open  
 Opens key: HKCR\exefile\shell\open  
 Opens key: HKCU\software\classes\exefile\shell\open\command  
 Opens key: HKCR\exefile\shell\open\command  
 Opens key:  
 HKCU\software\microsoft\windows\currentversion\policies\explorer\restricttrun  
 Opens key: HKCU\software\classes\exefile\shell\open\ddeexec  
 Opens key: HKCR\exefile\shell\open\ddeexec  
 Opens key: HKCU\software\classes\applications\cmd.exe  
 Opens key: HKCR\applications\cmd.exe  
 Opens key: HKCU\software\microsoft\windows\shellnoam  
 Opens key: HKCU\software\microsoft\windows\shellnoam\muicache  
 Opens key: HKCU\software\microsoft\windows\shellnoam\muicache\  
 Opens key: HKLM\system\currentcontrolset\control\session manager\apppcrttdlls  
 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\cmd.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: HKCU\software\microsoft\windows\currentversion\explorer\shell folders

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmd.exe

Opens key: HKLM\software\microsoft\windows

Opens key: HKLM\software\microsoft\windows\html help

Opens key: HKLM\software\microsoft\windows\help

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

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

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: HKCU\software\microsoft\windows\currentversion\thememanager  
Opens key: HKCU\software\policies\microsoft\windows\system  
Opens key: HKLM\software\microsoft\command processor  
Opens key: HKCU\software\microsoft\command processor  
Opens key: HKLM\system\currentcontrolset\control\nls\locale  
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts  
Opens key: HKLM\system\currentcontrolset\control\nls\language groups  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\appcompatflags\custom\tasklist.exe  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\tasklist.exe  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\mpr.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\framedyn.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dbghelp.dll  
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder  
Opens key: HKLM\software\microsoft\wbem\cimom  
Opens key: HKLM\software\microsoft\ctf\compatibility\tasklist.exe  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\tasklist.exe\rpcthreadpoolthrottle  
Opens key: HKLM\system\currentcontrolset\control\lsa  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\xpssp2res.dll  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\treatas  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\inprocserver32  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\inprocserverx86  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\localserver32  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\inprochandler32  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\inprochandlerx86  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-  
00aa004b2e24}\localserver  
Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\wbemcomn.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\wbemprox.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\winsta.dll  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-  
00c04fb68820}\treatas  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-  
00c04fb68820}\inprocserver32  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-  
00c04fb68820}\inprocserverx86  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-  
00c04fb68820}\localserver32  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler32  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver  
Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver  
Opens key: HKCU\software\classes\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}  
Opens key: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}  
Opens key: HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}  
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}  
Opens key: HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32  
Opens key: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver  
Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\wbemsvc.dll  
Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}  
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}  
Opens key: HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32  
Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}  
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}  
Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32  
Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver  
Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\msvc60.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\wldap32.dll  
Opens key: HKLM\system\currentcontrolset\services\ldap  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\ntdsapi.dll  
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\fastprox.dll  
Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-000000000001}

Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}  
Opens key: HKCU\software\classes\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32  
Opens key: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86  
Opens key: HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver  
Opens key: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver  
Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}  
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}  
Opens key: HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32  
Opens key: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32  
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd}  
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}  
Opens key: HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32  
Opens key: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32  
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\terminal server[tsuserenabled]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]  
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[6f21fb21650da014d87426fa0bd8e7f2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\imecompatibility[6f21fb21650da014d87426fa0bd8e7f2]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit\_dlls]  
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: 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[interfacehelperdisabletypelib]  
 Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]  
 Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]  
 Queries value: HKCU\control panel\desktop[multiuilanguageid]  
 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\system\currentcontrolset\control\session  
 manager[safeprocesssearchmode]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]  
 Queries value: HKCU\software\microsoft\ctf[disable thread input manager]  
 Queries value: HKLM\system\currentcontrolset\control\nls\codepage[932]  
 Queries value: HKLM\system\currentcontrolset\control\nls\codepage[949]  
 Queries value: HKLM\system\currentcontrolset\control\nls\codepage[950]  
 Queries value: HKLM\system\currentcontrolset\control\nls\codepage[936]  
 Queries value: HKLM\software\microsoft\com3[com+enabled]  
 Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]  
 Queries value: HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]  
 Queries value: HKLM\software\microsoft\com3[regdbversion]  
 Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]  
 Queries value: HKCU\control panel\desktop[smoothscroll]  
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]  
 Queries value: HKLM\software\microsoft\windows\currentversion\internet  
 settings[disableimprovedzonecheck]  
 Queries value: HKLM\software\microsoft\internet  
 explorer\main\featurecontrol\feature\_protocol\_lockdown[6f21fb21650da014d87426fa0bd8e7f2.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[disablebasicoverclearchannel]  
 Queries value: HKCU\software\microsoft\internet  
 explorer\main\featurecontrol[feature\_clientauthcertfilter]  
 Queries value: HKLM\software\microsoft\internet  
 explorer\main\featurecontrol[feature\_clientauthcertfilter]  
 Queries value: HKCU\software\microsoft\windows\currentversion\internet  
 settings[clientauthbuiltinui]  
 Queries value: HKCU\software\microsoft\windows\currentversion\internet  
 settings[syncmode5]

Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache[sessionstarttimedefaultdeltasecs]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache[signature]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings\5.0\cache\content[peruseritem]  
Queries value: HKLM\system\setup[systemsetupinprogress]  
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]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\domstore[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\feedplat[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\iecompat[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\ietld[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet settings\5.0\cache\extensible cache\mshist012014033120140407[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet

settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacherepair]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacheopath]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacheprefix]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cachelimit]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\5.0\cache\extensible cache\privacie:[cacheoptions]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disableworkerthreadhibernation]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[disableworkerthreadhibernation]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablereadrange]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[socketsendbufferlength]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[socketreceivebufferlength]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[keepalivetimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[maxhttpredirects]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[maxconnectionsperserver]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[maxconnectionsperserver]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[maxconnectionsper1\_0server]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[maxconnectionsper1\_0server]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[maxconnectionsperproxy]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[serverinfotimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[connecttimeout]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[connecttimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[connectretries]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[connectretries]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[sendtimeout]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[sendtimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[receivetimeout]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[receivetimeout]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[disablentlmpreauth]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[scavengecachelowerbound]  
Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings[certachenovalidate]  
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[6f21fb21650da014d87426fa0bd8e7f2.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[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[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:

[illegible]

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\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\internet  
explorer\main\featurecontrol\feature\_mime\_handling[6f21fb21650da014d87426fa0bd8e7f2.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[6f21fb21650da014d87426fa0bd8e7f2.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[6f21fb21650da014d87426fa0bd8e7f2.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}[leaseTerminateTime]  
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}[maxNumberOfAddressesToRegister]  
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[dnsNbTLookupOrder]  
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:      HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Queries value:      HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
  Queries value:      HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{11016101-e366-4d22-bc06-4ada335c892b}[suppressionpolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{1f4de370-d627-11d1-ba4f-00a0c91eedba}[suppressionpolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{450d8fba-ad25-11d0-98a8-0800361b1103}[suppressionpolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{645ff040-5081-101b-9f08-00aa002f954e}[suppressionpolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{e17d4fc0-5564-11d1-83f2-00a0c90dc849}[suppressionpolicy]
  Queries value:      HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value:      HKCR\clsid\{208d2c60-3aea-1069-a2d7-08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value:      HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\shellfolder[wantsparsedisplayname]
  Queries value:      HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[]
  Queries value:      HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}\inprocserver32[loadwithoutcom]
  Queries value:      HKLM\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Queries value:      HKCU\software\microsoft\windows\currentversion\shell
extensions\blocked[{871c5380-42a0-1069-a2ea-08002b30309d}]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[enforceshellextensionsecurity]

```

Queries value: HKLM\software\microsoft\windows\currentversion\shell  
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}  
0x401]

Queries value: HKCU\software\microsoft\windows\currentversion\shell  
extensions\cached[{871c5380-42a0-1069-a2ea-08002b30309d} {000214e6-0000-0000-c000-000000000046}  
0x401]

Queries value: HKLM\system\currentcontrolset\control\session  
manager\appcompatibility[disableappcompat]

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-  
08002b30309d}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-08002b30309d}[appid]

Queries value: HKCR\clsid\{871c5380-42a0-1069-a2ea-  
08002b30309d}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\windows\currentversion\app\_paths\iexplore.exe[]

Queries value: HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]

Queries value: HKLM\software\microsoft\internet  
explorer\setup[iexplorelastmodifiedhigh]

Queries value: HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]

Queries value: HKLM\software\microsoft\internet explorer\setup[installstarted]

Queries value: HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]

Queries value: HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]

Queries value: HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32[]

Queries value: HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]

Queries value: HKCR\clsid\{11016101-e366-4d22-bc06-  
4ada335c892b}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{1f4de370-d627-11d1-ba4f-  
00a0c91eedba}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{450d8fba-ad25-11d0-98a8-  
0800361b1103}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{645ff040-5081-101b-9f08-  
00aa002f954e}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{e17d4fc0-5564-11d1-83f2-  
00a0c90dc849}\shellfolder[wantsparsedisplayname]

Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]

Queries value: HKCR\clsid\{aeb6717e-7e19-11d0-97ee-  
00c04fd91972}\inprocserver32[loadwithoutcom]

Queries value: HKCR\ .exe[]

Queries value: HKCR\ .asp[]

Queries value: HKCR\ .bat[]

Queries value: HKCR\ .cer[]

Queries value: HKCR\ .chm[]

Queries value: HKCR\ .cmd[]

Queries value: HKCR\ .com[]

Queries value: HKCR\ .cpl[]

Queries value: HKCR\ .crt[]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-  
00c04fb6bfc4}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]

Queries value: HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-  
00c04fb6bfc4}\inprocserver32[threadingmodel]

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

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

Queries value: HKCU\software\microsoft\windows\currentversion\internet  
settings\zones\0[1806]

Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]

Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]

Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]

Queries value: HKLM\system\wpa\pnp[seed]

Queries value: HKLM\system\setup[osloaderpath]

Queries value: HKLM\system\setup[systempartition]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]

Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]

Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-  
11e3-9fc7-806d6172696f}[data]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-  
11e3-9fc7-806d6172696f}[generation]

Queries value: HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-  
409d6c4515e9}[drivemask]

Queries value:

HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]  
Queries value: HKCR\directory[docobject]  
Queries value: HKCR\directory[browseinplace]  
Queries value: HKCR\directory[isshortcut]  
Queries value: HKCR\directory[alwaysshowext]  
Queries value: HKCR\directory[nevershowext]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]  
Queries value: HKCR\exefile[docobject]  
Queries value: HKCR\exefile[browseinplace]  
Queries value: HKCR\exefile[isshortcut]  
Queries value: HKCR\exefile[alwaysshowext]  
Queries value: HKCR\exefile[nevershowext]  
Queries value: HKCR\exefile\shell[]  
Queries value: HKCR\exefile\shell\open\command[]  
Queries value: HKCR\exefile\shell\open\command[command]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[flags]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[state]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[userpreference]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[centralprofile]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileloadtimelow]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileloadtimehigh]  
Queries value: HKCU\software\microsoft\windows\shellnoroam\muicache[langid]  
Queries value:  
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\cmd.exe]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]  
Queries value:  
HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]  
Queries value: HKLM\system\wpa\mediacenter[installed]  
Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]  
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}[itemsizes]  
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[logfile]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]  
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[fdsupport]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]  
Queries value:  
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]  
Queries value:

[illegible]

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: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]  
 Queries value: HKCU\control panel\desktop[lamebuttontext]  
 Queries value: HKLM\software\microsoft\command processor[disableunccheck]  
 Queries value: HKLM\software\microsoft\command processor[enableextensions]  
 Queries value: HKLM\software\microsoft\command processor[delayedexpansion]  
 Queries value: HKLM\software\microsoft\command processor[defaultcolor]  
 Queries value: HKLM\software\microsoft\command processor[completionchar]  
 Queries value: HKLM\software\microsoft\command processor[pathcompletionchar]  
 Queries value: HKLM\software\microsoft\command processor[autorun]  
 Queries value: HKCU\software\microsoft\command processor[disableunccheck]  
 Queries value: HKCU\software\microsoft\command processor[enableextensions]  
 Queries value: HKCU\software\microsoft\command processor[delayedexpansion]  
 Queries value: HKCU\software\microsoft\command processor[defaultcolor]  
 Queries value: HKCU\software\microsoft\command processor[completionchar]  
 Queries value: HKCU\software\microsoft\command processor[pathcompletionchar]  
 Queries value: HKCU\software\microsoft\command processor[autorun]  
 Queries value: HKLM\system\currentcontrolset\control\locale\00000409  
 Queries value: HKLM\system\currentcontrolset\control\locale\language groups[1]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\compatibility32[tasklist]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime  
 compatibility[tasklist]  
 Queries value: HKLM\software\microsoft\wbem\cimom[logging]  
 Queries value: HKLM\software\microsoft\wbem\cimom[logging directory]  
 Queries value: HKLM\software\microsoft\wbem\cimom[log file max size]  
 Queries value: HKLM\software\microsoft\vol[maximumallowedallocationsize]  
 Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]  
 Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-  
 00aa004b2e24}\inprocserver32[inprocserver32]  
 Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]  
 Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]  
 Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-  
 00aa004b2e24}\inprocserver32[threadingmodel]  
 Queries value: HKLM\software\microsoft\wbem\cimom[repository directory]  
 Queries value: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]  
 Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]  
 Queries value: HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]  
 Queries value: HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]  
 Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-  
 00aa004b2e24}\inprocserver32[inprocserver32]  
 Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]  
 Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]  
 Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-  
 00aa004b2e24}\inprocserver32[threadingmodel]  
 Queries value: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]  
 Queries value: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]  
 Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-  
 ce99a996d9ea}\inprocserver32[inprocserver32]  
 Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]  
 Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]  
 Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-  
 ce99a996d9ea}\inprocserver32[threadingmodel]  
 Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]  
 Queries value: HKLM\software\microsoft\wbem\cimom[processid]  
 Queries value: HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]  
 Queries value: HKLM\software\microsoft\wbem\cimom[contextlimit]  
 Queries value: HKLM\software\microsoft\wbem\cimom[objectlimit]  
 Queries value: HKLM\software\microsoft\wbem\cimom[identifierlimit]  
 Queries value: HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32[]  
 Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-  
 00104b703efd}\inprocserver32[inprocserver32]  
 Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]  
 Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]  
 Queries value: HKCR\clsid\{1b1cad8c-2dab-11d2-b604-  
 00104b703efd}\inprocserver32[threadingmodel]  
 Queries value: HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]  
 Queries value: HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]  
 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]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
```