

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1247, Task ID: 4213	
Task ID:	4213
Risk Level:	5
Date Processed:	2016-07-12 05:10:25 (UTC)
Processing Time:	61.13 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\RajivApp1.exe"
Sample ID:	1247
Type:	basic
Owner:	admin
Label:	RajivApp1.exe
Date Added:	2016-07-12 05:10:24 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	8704 bytes
MD5:	9bde8983ac767c24755443627cda99bc
SHA256:	ca0dcf72ce74fa1084255dae79a6a787eccf04152cfadd23f775a1671f1149cf
Description:	None

Pattern Matching Results

- 4 Reads process memory
- 2 Resolves local hostname
- 2 .NET compiled executable
- 3 Long sleep detected
- 5 Query DNS from command line
- 4 Terminates process under Windows subfolder

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\RajivApp1.exe ["c:\windows\temp\RajivApp1.exe"]
Creates process:	C:\WINDOWS\system32\cmd.exe ["cmd.exe"]
Creates process:	C:\WINDOWS\system32\nslookup.exe [nslookup WORKGROUP]
Creates process:	C:\WINDOWS\system32\nslookup.exe [nslookup __MSBROWSE__]
Reads from process:	PID:288 C:\WINDOWS\system32\nslookup.exe
Reads from process:	PID:712 C:\WINDOWS\system32\nslookup.exe
Terminates process:	C:\WINDOWS\system32\nslookup.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	MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\SHIMLIB_LOG_Mutex
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.ELH
Creates event:	\BaseNamedObjects\CorDBIPCSyncSetupSyncEvent_1400
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore:	\BaseNamedObjects\GdiplusFontCacheFileV1

File System Events

Opens:	C:\WINDOWS\Prefetch\RAJIVAPP1.EXE-0FE9BC5A.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\mscoree.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\windows\temp\RajivApp1.exe.config
Opens:	C:\WINDOWS\Temp\RajivApp1.exe
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorlib.2.Manifest
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorlib.2.Config
Opens:	
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca	
Opens:	
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca\msvcr80.dll	
Opens:	C:\
Opens:	C:\WINDOWS
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config
Opens:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
Opens:	

C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\shell32.dll.124.Manifest
Opens: C:\WINDOWS\system32\shell32.dll.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security Config\v2.0.50727.42\security.config
Opens: C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security Config\v2.0.50727.42\security.config.cch
Opens: C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\index9c.dat
Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\mscorlib\9adb89fa22fd5b4ce433b5aca7fb1b07\mscorlib.ni.dll
Opens: C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
Opens: C:\WINDOWS\Temp
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\l_intl.nls
Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll.2.Manifest
Opens: C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll.2.Config
Opens: C:\WINDOWS\assembly\pubpol1.dat
Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System\aa7926460a336408c8041330ad90929d\System.ni.dll
Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Drawing\6978f2e90f13bc720d57fa6895c911e2\System.Drawing.ni.dll
Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\9a254c455892c02355ab0ab0f0727c5b\System.Windows.Forms.ni.dll
Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089
Opens: C:\WINDOWS\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089
Opens: C:\WINDOWS\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll.101.Manifest
Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll.101.Config
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c
Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.GdiPlus_6595b64144ccf1df_1.0.2600.5512_x-ww_dfb54e0c\GdiPlus.dll
Opens: C:\WINDOWS\system32\MSCTIME.IME
Opens: C:\Documents and Settings\Admin\Local Settings\Application Data\GDIPFONTCACHEV1.DAT
Opens: C:\WINDOWS\Fonts\micross.ttf
Opens: C:\WINDOWS\system32\cmd.exe
Opens: C:\WINDOWS\system32\apphelp.dll
Opens: C:\WINDOWS\AppPatch\sysmain.sdb
Opens: C:\WINDOWS\AppPatch\sysrest.sdb
Opens: C:\WINDOWS\system32
Opens: C:\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\winmm.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\ctype.nls
Opens:	C:\WINDOWS\system32\sortkey.nls
Opens:	C:\WINDOWS\system32\wbem\wmic.exe
Opens:	C:\WINDOWS\system32\winlogon.exe
Opens:	C:\WINDOWS\system32\xp2res.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\Documents and Settings
Opens:	C:\WINDOWS\system32\nslookup.exe
Opens:	C:\WINDOWS\system32\nslookup.exe.Manifest
Opens:	C:\WINDOWS\Prefetch\NSLOOKUP.EXE-160B1221.pf
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\mswsock.dll
Opens:	C:\WINDOWS\system32\dnsapi.dll
Opens:	C:\WINDOWS\system32\iphlpapi.dll
Opens:	C:\WINDOWS\system32\winnr.dll
Opens:	C:\WINDOWS\system32\hnetcfg.dll
Opens:	C:\WINDOWS\system32\wshtcpip.dll
Opens:	C:\WINDOWS\system32\MSIMTF.dll
Reads from:	C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Reads from:	C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

Network Events

DNS query:	8.8.8.8.in-addr.arpa
DNS query:	WORKGROUP
DNS query:	_MSBROWSE_
Connects to:	8.8.8.8:53
Sends data to:	8.8.8.8:53

Windows Registry Events

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\fusion\gacchangenotification\default
Creates key:	HKCU\software\microsoft\gdipplus
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\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\rajivapp1.exe
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\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\session manager
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\ntdll.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\mscoree.dll
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:	HKLM\software\microsoft\.netframework
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
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\gdi32.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\shlwapi.dll
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument
Opens key:	HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:	HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:	HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key:	HKCU\

Opens key: HKCU\software\microsoft\.netframework\policy\standards
 Opens key: HKLM\software\microsoft\.netframework\policy\standards
 Opens key: HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
 Opens key: HKCU\software\policies\microsoft\control panel\desktop
 Opens key: HKCU\control panel\desktop
 Opens key:
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msvcr80.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\mscorwks.dll
 Opens key: HKCU\software\microsoft\.netframework
 Opens key: HKLM\software\microsoft\fusion
 Opens key: HKCU\software\microsoft\fusion
 Opens key:
 HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets
 Opens key:
 HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
 Opens key:
 HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\localintranet
 Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
 1757981266-507921405-1957994488-1003
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\shell32.dll
 Opens key: HKLM\system\setup
 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\.netframework\v2.0.50727\security\policy
 Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32
 Opens key: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8
 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\mscorlib.ni.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msctf.dll
 Opens key: HKLM\software\microsoft\ctf\compatibility\rajivapp1.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\fusion\nativeimagesindex\v2.0.50727_32\ni\38c56119\1d3ee2d7
 Opens key: HKLM\software\microsoft\net framework setup\dotnetclient\v3.5
 Opens key: HKLM\software\microsoft\strongname
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\mscorlibjit.dll
 Opens key: HKLM\software\microsoft\fusion\publisherpolicy\default
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\1d
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17
 Opens key:
 HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\1e
 Opens key: HKLM\software\microsoft\.netframework\policy\aptca
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\uxtheme.dll
 Opens key: HKCU\software\microsoft\windows\currentversion\thememanager

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.ni.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.drawing.ni.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.windows.forms.ni.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdiplus.dll
Opens key: HKLM\hardware\devicemap\video
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: HKLM\software\microsoft\windows nt\currentversion\fonts
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key: HKCU\udc\1252
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
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\session manager\appcertdlls
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
Opens key: HKLM\system\wpa\tabletpc
Opens key: HKLM\system\wpa\mediacenter
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\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\rpc\pagedbuffers
 Opens key: HKLM\software\microsoft\rpc
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rajivapp1.exe\rpc\threadpoolthrottle
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKCU\software\classes\
 Opens key: HKCU\software\classes\appid\rajivapp1.exe
 Opens key: HKCR\appid\rajivapp1.exe
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\currentcontrolset\control\lsa
 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\winmm.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

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

options\userenv.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\oleaut
 Opens key: HKLM\software\microsoft\oleaut\userera
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache
 Opens key:

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

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\xpssp2res.dll
 Opens key:

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
 Opens key:

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

HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
 Opens key: HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
 Opens key: HKLM\system\currentcontrolset\control\mediaresources\acm
 Opens key: HKLM\system\currentcontrolset\control\productoptions
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders
 Opens key: HKLM\software\policies\microsoft\windows\system
 Opens key: HKCU\software\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\sllookup.exe
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\sllookup.exe
 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\software\microsoft\windows nt\currentversion\image file execution

options\wssock32.dll
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

options\dnsapi.dll
 Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
 Opens key: HKLM\system\currentcontrolset\services\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: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\nslookup.exe\rpcthreadpoolthrottle
 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\windows nt\currentversion\image file execution

options\ldap32.dll
 Opens key: HKLM\system\currentcontrolset\services\ldap
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

options\hnetcfg.dll
 Opens key: HKLM\software\microsoft\rpc\securityservice
 Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wshtcpip.dll
 Opens key: HKCU\software\microsoft\ctf\langbaraddin\
 Opens key: HKLM\software\microsoft\ctf\langbaraddin\
 Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\mscoree.dll[checkapphelp]
 Queries value: HKLM\system\currentcontrolset\control\session manager\appcompatibility[disableappcompat]
 Queries value: HKLM\software\microsoft\.netframework[installroot]
 Queries value: HKLM\software\microsoft\.netframework[clrloadlogdir]
 Queries value: HKLM\software\microsoft\.netframework[onlyuselatestclr]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[rajivapp1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[rajivapp1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorwks.dll[checkapphelp]
Queries value: HKLM\software\microsoft\.netframework[gcstresstart]
Queries value: HKLM\software\microsoft\.netframework[gcstresstartatjit]
Queries value: HKLM\software\microsoft\.netframework[disableconfigcache]
Queries value: HKLM\software\microsoft\fusion[cacheolocation]
Queries value: HKLM\software\microsoft\fusion[downloadcachequotainkb]
Queries value: HKLM\software\microsoft\fusion[enablelog]
Queries value: HKLM\software\microsoft\fusion[logginglevel]
Queries value: HKLM\software\microsoft\fusion[forceolog]
Queries value: HKLM\software\microsoft\fusion[logfailures]
Queries value: HKLM\software\microsoft\fusion[versioninglog]
Queries value: HKLM\software\microsoft\fusion[logresourcebinds]
Queries value: HKLM\software\microsoft\fusion[uselegacyidentityformat]
Queries value: HKLM\software\microsoft\fusion[disablemsipeek]
Queries value: HKLM\software\microsoft\fusion[noclientchecks]
Queries value: HKLM\system\setup\systemsetupinprogress]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c[niusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c[ilusagemask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[evaluationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
Queries value: HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperperisableall]
Queries value: HKCR\interface[interfacehelperperisableallforole32]
Queries value: HKCR\interface[interfacehelperperisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperperisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperperisableallforole32]
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: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[index1]
Queries value:
HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configmask]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configmask]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\7e[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\7e[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\7e[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\7e[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\7e[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[accessibility,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttoncontext]
Queries value: HKLM\software\microsoft\.netframework[dbgjitdebuglaunchsetting]
Queries value: HKLM\software\microsoft\.netframework[dbgmanageddebugger]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\gdiplus[fontcachepath]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
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\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[cmd]
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]

[illegible]

Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
Queries value: HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
Queries value: HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
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\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\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[nslookup]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[nslookup]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]

Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlDs]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[useDns]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatezoneexcludefile]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updateopleveldomainzones]
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\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:

[illegible]

Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]
 Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\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}[maxnumberofaddressesstoregister]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters[dnsbtlookuporder]
 Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
 Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
 Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
 Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
 Queries value:
 HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
 Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell
 folders[appdata]
 Value changes: HKLM\software\microsoft\cryptography\rng[seed]
 Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell
 folders[cache]