Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1167, Task ID: 4096

Task ID:	4096
Risk Level:	5
Date Processed:	2016-07-04 04:18:06 (UTC)
Processing Time:	63.29 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\RajivApp1.exe"
Sample ID:	1167
Type:	basic
Owner:	admin
Label:	RajivApp1.exe
Date Added:	2016-07-04 04:18:06 (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:2588 C:\Windows\System32\nslookup.exe
Reads from process:	PID:2628 C:\Windows\System32\nslookup.exe
Terminates process:	C:\Windows\System32\nslookup.exe
Terminates process:	C:\Windows\System32\cmd.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\BaseNamedObjects\CorDBIPCSetupSyncEvent_2484
Creates event:	\KernelObjects\LowMemoryCondition
Creates event:	\BaseNamedObjects\ConsoleEvent-0x00000A10
Creates event:	\BaseNamedObjects\ConsoleEvent-0x00000A38
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates semaphore:	\Sessions\1\BaseNamedObjects\GdiplusFontCacheFileV1

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Creates:	C:\Users\Admin\AppData\Local\GDIPFONTCACHEV1.DAT
Opens:	C:\Windows\Prefetch\RAJIVAPP1.EXE-4C2BBC3A.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\mscoree.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\SYSTEM32\MSCOREE.DLL.local
Opens:	C:\Windows\Microsoft.NET\Framework\v2.0.50727
Opens:	C:\Windows\Microsoft.NET\Framework\Upgrades.2.0.50727\
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\mscorwks.dll
Opens:	C:\windows\temp\RajivApp1.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
Opens:	C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\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\fusion.localgac
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\Globalization\Sorting\SortDefault.nls
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\System32\profapi.dll
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
Opens: C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\index145.dat
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
Opens: C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
Opens: C:\Windows\Temp
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\windows\temp\CRYPTBASE.dll
Opens: C:\Windows\System32\cryptbase.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files
Opens: C:\windows\temp\RajivApp1.config
Opens: C:\Windows\System32\l_intl.nls
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
Opens: C:\Windows\assembly\pubpol4.dat
Opens: C:\Windows\assembly\GAC\PublisherPolicy.tme
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
Opens: C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\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\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\uxtheme.dll
Opens: C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
Opens: C:\Windows\Globalization\en-us.nlp
Opens: C:\Windows\Microsoft.NET\Framework\v2.0.50727\Gdiplus.dll
Opens: C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
Opens: C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
Opens: C:\Users\Admin\AppData\Local\GDIPFONTCACHEV1.DAT
Opens: C:\Windows\Fonts\marlett.ttf
Opens: C:\Windows\Fonts\arial.ttf
Opens: C:\Windows\Fonts\ariali.ttf
Opens: C:\Windows\Fonts\arialbd.ttf
Opens: C:\Windows\Fonts\arialbi.ttf
Opens: C:\Windows\Fonts\batang.ttc
Opens: C:\Windows\Fonts\cour.ttf
Opens: C:\Windows\Fonts\couri.ttf
Opens: C:\Windows\Fonts\courbd.ttf
Opens: C:\Windows\Fonts\courbi.ttf
Opens: C:\Windows\Fonts\daunpenh.ttf
Opens: C:\Windows\Fonts\dokchamp.ttf
Opens: C:\Windows\Fonts\estre.ttf
Opens: C:\Windows\Fonts\euphemia.ttf
Opens: C:\Windows\Fonts\gautami.ttf
Opens: C:\Windows\Fonts\gautamib.ttf
Opens: C:\Windows\Fonts\Vani.ttf
Opens: C:\Windows\Fonts\Vanib.ttf
Opens: C:\Windows\Fonts\gulim.ttc
Opens: C:\Windows\Fonts\impact.ttf
Opens: C:\Windows\Fonts\iskpota.ttf
Opens: C:\Windows\Fonts\iskpotab.ttf
Opens: C:\Windows\Fonts\kalinga.ttf
Opens: C:\Windows\Fonts\kalingab.ttf
Opens: C:\Windows\Fonts\kartika.ttf
Opens: C:\Windows\Fonts\kartikab.ttf
Opens: C:\Windows\Fonts\KhmerUI.ttf
Opens: C:\Windows\Fonts\KhmerUIb.ttf
Opens: C:\Windows\Fonts\LaoUI.ttf
Opens: C:\Windows\Fonts\LaoUIb.ttf
Opens: C:\Windows\Fonts\latha.ttf
Opens: C:\Windows\Fonts\lathab.ttf
Opens: C:\Windows\Fonts\lucon.ttf
Opens: C:\Windows\Fonts\malgun.ttf
Opens: C:\Windows\Fonts\malgunbd.ttf
Opens: C:\Windows\Fonts\mangal.ttf
Opens: C:\Windows\Fonts\mangalb.ttf
Opens: C:\Windows\Fonts\meiryo.ttc
Opens: C:\Windows\Fonts\meiryob.ttc
Opens: C:\Windows\Fonts\himalaya.ttf
Opens: C:\Windows\Fonts\msjh.ttf
Opens: C:\Windows\Fonts\msjhbd.ttf

Opens: C:\Windows\Fonts\msyh.ttf
Opens: C:\Windows\Fonts\msyhbd.ttf
Opens: C:\Windows\Fonts\mingliu.ttc
Opens: C:\Windows\Fonts\mingliub.ttc
Opens: C:\Windows\Fonts\monbaiti.ttf
Opens: C:\Windows\Fonts\msgothic.ttc
Opens: C:\Windows\Fonts\msmincho.ttc
Opens: C:\Windows\Fonts\mvboli.ttf
Opens: C:\Windows\Fonts\ntailu.ttf
Opens: C:\Windows\Fonts\ntailub.ttf
Opens: C:\Windows\Fonts\nyala.ttf
Opens: C:\Windows\Fonts\phagspa.ttf
Opens: C:\Windows\Fonts\phagspab.ttf
Opens: C:\Windows\Fonts\plantc.ttf
Opens: C:\Windows\Fonts\raavi.ttf
Opens: C:\Windows\Fonts\raavib.ttf
Opens: C:\Windows\Fonts\segoesc.ttf
Opens: C:\Windows\Fonts\segoescb.ttf
Opens: C:\Windows\Fonts\segoeui.ttf
Opens: C:\Windows\Fonts\segoeuib.ttf
Opens: C:\Windows\Fonts\segoeuii.ttf
Opens: C:\Windows\Fonts\segoeuiz.ttf
Opens: C:\Windows\Fonts\seguisb.ttf
Opens: C:\Windows\Fonts\segoeuil.ttf
Opens: C:\Windows\Fonts\seguisym.ttf
Opens: C:\Windows\Fonts\shruti.ttf
Opens: C:\Windows\Fonts\shrutib.ttf
Opens: C:\Windows\Fonts\simsun.ttc
Opens: C:\Windows\Fonts\simsunb.ttf
Opens: C:\Windows\Fonts\sylfaen.ttf
Opens: C:\Windows\Fonts\taile.ttf
Opens: C:\Windows\Fonts\taileb.ttf
Opens: C:\Windows\Fonts\times.ttf
Opens: C:\Windows\Fonts\timesi.ttf
Opens: C:\Windows\Fonts\timesbd.ttf
Opens: C:\Windows\Fonts\timesbi.ttf
Opens: C:\Windows\Fonts\tunga.ttf
Opens: C:\Windows\Fonts\tungab.ttf
Opens: C:\Windows\Fonts\vrinda.ttf
Opens: C:\Windows\Fonts\vrindab.ttf
Opens: C:\Windows\Fonts\Shonar.ttf
Opens: C:\Windows\Fonts\Shonarb.ttf
Opens: C:\Windows\Fonts\msyi.ttf
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\Windows\Fonts\tahomabd.ttf
Opens: C:\Windows\Fonts\micross.ttf
Opens: C:\Windows\Fonts\angsa.ttf
Opens: C:\Windows\Fonts\angsai.ttf
Opens: C:\Windows\Fonts\angsab.ttf
Opens: C:\Windows\Fonts\angsaz.ttf
Opens: C:\Windows\Fonts\aparaj.ttf
Opens: C:\Windows\Fonts\aparajb.ttf
Opens: C:\Windows\Fonts\aparajbi.ttf
Opens: C:\Windows\Fonts\aparaji.ttf
Opens: C:\Windows\Fonts\cordia.ttf
Opens: C:\Windows\Fonts\cordiai.ttf
Opens: C:\Windows\Fonts\cordiab.ttf
Opens: C:\Windows\Fonts\cordiaz.ttf
Opens: C:\Windows\Fonts\ebrima.ttf
Opens: C:\Windows\Fonts\ebrimabd.ttf
Opens: C:\Windows\Fonts\gisha.ttf
Opens: C:\Windows\Fonts\gishabd.ttf
Opens: C:\Windows\Fonts\kokila.ttf
Opens: C:\Windows\Fonts\kokilab.ttf
Opens: C:\Windows\Fonts\kokilabi.ttf
Opens: C:\Windows\Fonts\kokilai.ttf
Opens: C:\Windows\Fonts\leelawad.ttf
Opens: C:\Windows\Fonts\leelawdb.ttf
Opens: C:\Windows\Fonts\msuighur.ttf
Opens: C:\Windows\Fonts\moolbor.ttf
Opens: C:\Windows\Fonts\symbol.ttf
Opens: C:\Windows\Fonts\utsaah.ttf
Opens: C:\Windows\Fonts\utsaahb.ttf
Opens: C:\Windows\Fonts\utsaahbi.ttf
Opens: C:\Windows\Fonts\utsaahi.ttf
Opens: C:\Windows\Fonts\vijaya.ttf
Opens: C:\Windows\Fonts\vijayab.ttf
Opens: C:\Windows\Fonts\wingding.ttf
Opens: C:\Windows\Fonts\modern.fon
Opens: C:\Windows\Fonts\roman.fon
Opens: C:\Windows\Fonts\script.fon
Opens: C:\Windows\Fonts\andlso.ttf
Opens: C:\Windows\Fonts\arabtype.ttf
Opens: C:\Windows\Fonts\simpo.ttf
Opens: C:\Windows\Fonts\simpbdo.ttf
Opens: C:\Windows\Fonts\simpfxo.ttf
Opens: C:\Windows\Fonts\majalla.ttf
Opens: C:\Windows\Fonts\majallab.ttf

Opens: C:\Windows\Fonts\trado.ttf
Opens: C:\Windows\Fonts\tradbdo.ttf
Opens: C:\Windows\Fonts\ahronbd.ttf
Opens: C:\Windows\Fonts\david.ttf
Opens: C:\Windows\Fonts\davidbd.ttf
Opens: C:\Windows\Fonts\frank.ttf
Opens: C:\Windows\Fonts\lvnm.ttf
Opens: C:\Windows\Fonts\lvnmbd.ttf
Opens: C:\Windows\Fonts\mriam.ttf
Opens: C:\Windows\Fonts\mriamc.ttf
Opens: C:\Windows\Fonts\nrkis.ttf
Opens: C:\Windows\Fonts\rod.ttf
Opens: C:\Windows\Fonts\simfang.ttf
Opens: C:\Windows\Fonts\simhei.ttf
Opens: C:\Windows\Fonts\simkai.ttf
Opens: C:\Windows\Fonts\angsau.ttf
Opens: C:\Windows\Fonts\angsaui.ttf
Opens: C:\Windows\Fonts\angsaub.ttf
Opens: C:\Windows\Fonts\angsauz.ttf
Opens: C:\Windows\Fonts\browa.ttf
Opens: C:\Windows\Fonts\browai.ttf
Opens: C:\Windows\Fonts\browab.ttf
Opens: C:\Windows\Fonts\browaz.ttf
Opens: C:\Windows\Fonts\browau.ttf
Opens: C:\Windows\Fonts\browaui.ttf
Opens: C:\Windows\Fonts\browaub.ttf
Opens: C:\Windows\Fonts\browauz.ttf
Opens: C:\Windows\Fonts\cordiau.ttf
Opens: C:\Windows\Fonts\cordiaub.ttf
Opens: C:\Windows\Fonts\cordiauz.ttf
Opens: C:\Windows\Fonts\cordiaui.ttf
Opens: C:\Windows\Fonts\upcdl.ttf
Opens: C:\Windows\Fonts\upcdi.ttf
Opens: C:\Windows\Fonts\upcdb.ttf
Opens: C:\Windows\Fonts\upcdbi.ttf
Opens: C:\Windows\Fonts\upcel.ttf
Opens: C:\Windows\Fonts\upcei.ttf
Opens: C:\Windows\Fonts\upceb.ttf
Opens: C:\Windows\Fonts\upcebi.ttf
Opens: C:\Windows\Fonts\upcfl.ttf
Opens: C:\Windows\Fonts\upcfi.ttf
Opens: C:\Windows\Fonts\upcfb.ttf
Opens: C:\Windows\Fonts\upcfbi.ttf
Opens: C:\Windows\Fonts\upcil.ttf
Opens: C:\Windows\Fonts\upcii.ttf
Opens: C:\Windows\Fonts\upcib.ttf
Opens: C:\Windows\Fonts\upcibi.ttf
Opens: C:\Windows\Fonts\upcjl.ttf
Opens: C:\Windows\Fonts\upcji.ttf
Opens: C:\Windows\Fonts\upcjb.ttf
Opens: C:\Windows\Fonts\upcjbi.ttf
Opens: C:\Windows\Fonts\upckl.ttf
Opens: C:\Windows\Fonts\upcki.ttf
Opens: C:\Windows\Fonts\upckb.ttf
Opens: C:\Windows\Fonts\upckbi.ttf
Opens: C:\Windows\Fonts\upcll.ttf
Opens: C:\Windows\Fonts\upcli.ttf
Opens: C:\Windows\Fonts\upclb.ttf
Opens: C:\Windows\Fonts\upclbi.ttf
Opens: C:\Windows\Fonts\kaiu.ttf
Opens: C:\Windows\Fonts\l_10646.ttf
Opens: C:\Windows\Fonts\ariblk.ttf
Opens: C:\Windows\Fonts\calibri.ttf
Opens: C:\Windows\Fonts\calibrii.ttf
Opens: C:\Windows\Fonts\calibrib.ttf
Opens: C:\Windows\Fonts\calibriz.ttf
Opens: C:\Windows\Fonts\cambria.ttc
Opens: C:\Windows\Fonts\cambriai.ttf
Opens: C:\Windows\Fonts\cambriab.ttf
Opens: C:\Windows\Fonts\cambriaz.ttf
Opens: C:\Windows\Fonts\Candara.ttf
Opens: C:\Windows\Fonts\Candarai.ttf
Opens: C:\Windows\Fonts\Candarab.ttf
Opens: C:\Windows\Fonts\Candaraz.ttf
Opens: C:\Windows\Fonts\comic.ttf
Opens: C:\Windows\Fonts\comicbd.ttf
Opens: C:\Windows\Fonts\consola.ttf
Opens: C:\Windows\Fonts\consolai.ttf
Opens: C:\Windows\Fonts\consolab.ttf
Opens: C:\Windows\Fonts\consolaz.ttf
Opens: C:\Windows\Fonts\constan.ttf
Opens: C:\Windows\Fonts\constani.ttf
Opens: C:\Windows\Fonts\constanb.ttf
Opens: C:\Windows\Fonts\constanz.ttf
Opens: C:\Windows\Fonts\corbel.ttf
Opens: C:\Windows\Fonts\corbeli.ttf
Opens: C:\Windows\Fonts\corbelb.ttf
Opens: C:\Windows\Fonts\corbelz.ttf

Opens: C:\Windows\Fonts\framd.ttf
Opens: C:\Windows\Fonts\framdit.ttf
Opens: C:\Windows\Fonts\Gabriola.ttf
Opens: C:\Windows\Fonts\georgia.ttf
Opens: C:\Windows\Fonts\georgiai.ttf
Opens: C:\Windows\Fonts\georgiab.ttf
Opens: C:\Windows\Fonts\georgiaz.ttf
Opens: C:\Windows\Fonts\pala.ttf
Opens: C:\Windows\Fonts\palai.ttf
Opens: C:\Windows\Fonts\palab.ttf
Opens: C:\Windows\Fonts\palabi.ttf
Opens: C:\Windows\Fonts\segoepr.ttf
Opens: C:\Windows\Fonts\segoeprb.ttf
Opens: C:\Windows\Fonts\trebuc.ttf
Opens: C:\Windows\Fonts\trebucit.ttf
Opens: C:\Windows\Fonts\trebucbd.ttf
Opens: C:\Windows\Fonts\trebucbi.ttf
Opens: C:\Windows\Fonts\verdana.ttf
Opens: C:\Windows\Fonts\verdanai.ttf
Opens: C:\Windows\Fonts\verdanab.ttf
Opens: C:\Windows\Fonts\verdanaz.ttf
Opens: C:\Windows\Fonts\webdings.ttf
Opens: C:\Windows\Fonts\coure.fon
Opens: C:\Windows\Fonts\serife.fon
Opens: C:\Windows\Fonts\sserife.fon
Opens: C:\Windows\Fonts\smalle.fon
Opens: C:\Windows\Fonts\smallf.fon
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\System32\dwmapi.dll
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\System32\en-US\user32.dll.mui
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\system32\uxtheme.dll.Config
Opens: C:\windows\temp\cmd.exe
Opens: C:\Windows\System32\cmd.exe
Opens: C:\Windows\System32\apphelp.dll
Opens: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
Opens: C:
Opens: C:\Program Files
Opens: C:\Program Files\Adobe
Opens: C:\Program Files\Adobe\Reader 9.0
Opens: C:\Program Files\Adobe\Reader 9.0\Reader
Opens: C:\Windows\Branding
Opens: C:\Windows\Branding\Basebrd
Opens: C:\Windows\Branding\Basebrd\en-US
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\System32\en-US
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\Windows\System32\apisetschema.dll
Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\System32\msvcrt.dll
Opens: C:\Windows\System32\winbrand.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\gdi32.dll
Opens: C:\Windows\System32\lpk.dll
Opens: C:\Windows\System32\usp10.dll
Opens: C:\Windows\System32\msctf.dll
Opens: C:\Windows\System32\en-US\cmd.exe.mui
Opens: C:\Windows\Branding\Basebrd\basebrd.dll
Opens: C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
Opens: C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
Opens: C:\windows\temp\CRYPTSP.dll
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.dll
Opens: C:\windows\temp\RpcRtRemote.dll
Opens: C:\Windows\System32\RpcRtRemote.dll
Opens: C:\Windows\system32\Branding\Basebrd\Basebrd.dll
Opens: C:\Windows\System32\nslookup.exe
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\Windows\system32\ui\SwDRM.dll
Opens: C:\Windows\Prefetch\NSLOOKUP.EXE-3DO6E09F.pf
Opens: C:\Windows\System32\wsock32.dll
Opens: C:\Windows\System32\mswsock.dll
Opens: C:\Windows\System32\dnsapi.dll
Opens: C:\Windows\System32\en-US\nslookup.exe.mui
Opens: C:\Windows\System32\WSHTCPIP.DLL
Opens: C:\Windows\System32\nlaapi.dll
Opens: C:\Windows\System32\NapiNSP.dll
Opens: C:\Windows\System32\pnrpnsp.dll
Opens: C:\Windows\System32\winrnr.dll
Opens: C:\Windows\System32\IPHLPAPI.DLL

Opens: C:\Windows\System32\winnsi.dll
Opens: C:\Windows\System32\dhcpcsvc6.dll
Opens: C:\Windows\System32\dhcpcsvc.dll
Reads from: C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
Reads from: C:\Windows\System32\nslookup.exe

Network Events

DNS query: 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
Receives data from: 8.8.8.8:53

Windows Registry Events

Creates key: HKLM\software\microsoft\fusion\gacchangenotification\default
Creates key: HKCU\software\microsoft\gdiplus
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\software\microsoft\.netframework\policy\
Opens key: HKLM\software\microsoft\.netframework\policy\v2.0
Opens key: HKLM\software\microsoft\.netframework
Opens key: HKLM\software\microsoft\.netframework\policy\upgrades
Opens key: HKLM\software\microsoft\.netframework\policy\standards
Opens key: HKLM\software\microsoft\.netframework\policy\apppatch
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: HKCU\software\microsoft\.netframework\policy\standards
Opens key: HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKCU\software\microsoft\.netframework
Opens key: HKLM\software\microsoft\fusion
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rajivapp1.exe
Opens key: HKCU\software\microsoft\fusion
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
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-1-5-21-2160590473-689474908-1361669368-1002
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}\propertybag
Opens key: HKCU\software\microsoft\windows\currentversion\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\policies\microsoft\windows\explorer

Opens key: HKCU\software\policies\microsoft\windows\explorer
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-
9afe-ea3317b67173}\propertybag
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings
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\index145
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\89
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-
ba85-6007caedcf9d}\propertybag
Opens key:
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\fusion\publisherpolicy\default
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.windows.forms__b77a5c561934e089
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\82
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83
Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.drawing__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system__b77a5c561934e089
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.xml__b77a5c561934e089
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.configuration__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.deployment__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.runtime.serialization.formatters.soap__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.accessibility__b03f5f7f11d50a3a
Opens key:
HKLM\software\microsoft\fusion\publisherpolicy\default\policy.2.0.system.security__b03f5f7f11d50a3a
Opens key: HKLM\software\microsoft\.netframework\policy\aptca
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000
Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&0&10
Opens key: HKLM\software\microsoft\windows nt\currentversion\fonts
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key: HKCU\eudc\1252
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
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\languagepack\datastore_v1.0

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmd.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\cmd.exe
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\appid\rajivapp1.exe
Opens key: HKCR\appid\rajivapp1.exe
Opens key: HKLM\software\microsoft\ole\appcompat
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}
Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\
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\software\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\nslookup.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\nslookup.exe
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2-3373a944
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\psched\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\system\currentcontrolset\services\dns
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-
c19ce8a73253}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-
806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{8ff7f47b-d658-4061-baea-
1709a0196aed}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{7b9cb019-1924-49a5-867c-
a68f334c8d34}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\microsoft sans serif
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\3a41eaa2-2d47c47e
Opens key: HKLM\software\microsoft\ctf\compatibility\rajivapp1.exe
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\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\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\.netframework[gcstressstart]
Queries value: HKLM\software\microsoft\.netframework[gcstressstartatjit]
Queries value: HKLM\software\microsoft\.netframework[disableconfigcache]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[e13c0d23-ccbc-4e12-931b-d9cc2eee27e4]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[cc2bcbba-16b6-4cf3-8990-d74c2e8af500]
Queries value: HKLM\software\microsoft\fusion[cachelocation]
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[forcelog]
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\software\microsoft\windows nt\currentversion\image file execution options[devoverrideenable]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[category]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[name]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parentfolder]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[description]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[relativepath]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[parsingname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[infotip]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localizedname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[security]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresource]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[streamresourcetype]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[localredirectonly]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[roamable]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[precreate]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[stream]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[publishexpandedpath]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[attributes]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[foldertypeid]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{3eb685db-65f9-4cf6-a03a-e3ef65729f3d}[initfolderhandler]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[category]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[name]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parentfolder]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[description]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[relativepath]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[parsingname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[infotip]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localizedname]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[icon]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[security]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresource]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[streamresourcetype]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[localredirectonly]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[roamable]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[precreate]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[stream]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[publishexpandedpath]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[attributes]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[foldertypeid]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{5e6c858f-0e22-4760-9afe-ea3317b67173}[initfolderhandler]
Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-2160590473-689474908-1361669368-1002[profileimagepath]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index145[niusagemask]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index145[ilusagemask]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[displayname]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[configmask]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[configstring]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[mvid]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[evalationdata]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[status]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[ildependencies]
Queries value: HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[nidependencies]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\89[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\183e33de\89[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[category]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[name]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parentfolder]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[description]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[relativepath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[parsingname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[infotip]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localizedname]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[icon]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[security]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresource]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[streamresourcetype]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[localredirectonly]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[roamable]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[precreate]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[stream]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[publishexpandedpath]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[attributes]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[foldertypeid]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{352481e8-33be-4251-ba85-6007caedcf9d}[initfolderhandler]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[cache]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
Queries value: HKLM\software\microsoft\fusion\publisherpolicy\default[index4]
Queries value:
HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[mvid]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\82[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\2d382ce6\8c[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\1bd7b0d8\8e[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\163e1f5e\88[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\1c83327b\8d[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\7f3b6ac4\80[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\1b2590b1\84[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\2bd33e1c\81[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[mvid]

Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\8f[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\6f1da7aa\8f[lastmodtime]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[configmask]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[configstring]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[mvid]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[evalationdata]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[ildependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[nidependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\83[missingdependencies]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86[displayname]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86[status]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86[modules]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86[sig]
Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\a5cd4db\86[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: 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\video3]
Queries value: HKLM\system\currentcontrolset\control\video\{c54b6caf-be91-4a10-ab56-
fd27e3774e32}\0000[pruningmode]
Queries value: HKCU\software\microsoft\gdiplus[fontcachepath]
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\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]
Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[76c7ff28]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
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\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\layers[c:\windows\system32\nslookup.exe]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[nslookup]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dnslookuporder]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpdomain]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[dhcpsearchlist]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enabledaforallnetworks]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccessqueryorder]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]

Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[cacheallcompartments]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usenewregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[resolverregistrationonly]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpv6domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[dhcpnameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{128919e8-8a5e-41d1-ac17-c19ce8a73253}[enablemulticast]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{e29ac6c2-7037-11de-816d-806e6f6e6963}[enablemulticast]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]