Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	4094
Risk Level:	5
Date Processed:	2016-07-04 04:18:06 (UTC)
Processing Time:	62.47 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

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

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:	\SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
Creates process:	C:\Windows\system32\nslookup.exe [nslookup WORKGROUP]
Creates process:	C:\Windows\system32\nslookup.exe [nslookup __MSBROWSE__]
Reads from process:	PID:856 C:\Windows\System32\nslookup.exe
Reads from process:	PID:1592 C:\Windows\System32\nslookup.exe
Terminates process:	C:\Windows\System32\nslookup.exe
Terminates process:	C:\Windows\System32\cmd.exe
Terminates process:	C:\Windows\System32\conhost.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\CorDBIPCSetupSyncEvent_3004

File System Events

Creates:	C:\Users\Admin
Creates:	C:\Users\Admin\AppData\Roaming
Opens:	C:\Windows\Prefetch\RAJIVAPP1.EXE-4C2BBC3A.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\mscoree.dll
Opens:	C:\Windows\System32\apphelp.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\Windows\Temp\RajivApp1.exe
Opens:	C:\Windows\System32\ntdll.dll
Opens:	C:\Windows\System32\kernel32.dll
Opens:	C:\Windows\System32\KernelBase.dll
Opens:	C:\Windows\System32\msvcrt.dll
Opens:	C:\Windows\apppatch\apppatch64\sysmain.sdb
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\rpcrt4.dll
Opens:	C:\Windows\System32\advapi32.dll
Opens:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319
Opens:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
Opens:	C:\Windows\Microsoft.NET\Framework64
Opens:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\clr.dll
Opens:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
Opens:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\clr.dll
Opens:	C:\Windows\System32\gdi32.dll
Opens:	C:\Windows\System32\user32.dll
Opens:	C:\Windows\System32\shlwapi.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\msctf.dll
Opens:	C:\windows\temp\RajivApp1.exe.config
Opens:	C:\Windows\WinSxS\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_88dc8c812fb1ba3f
Opens:	C:\Windows\WinSxS\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.6910_none_88dc8c812fb1ba3f\msvcr80.dll
Opens:	C:\
Opens:	C:\Windows
Opens:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
Opens:	

```
C:\Users\Admin\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\RajivApp1.exe.log
  Opens:                  C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\security.config
  Opens:
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\security.config.cch
  Opens:
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config
  Opens:
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\config\enterprisesec.config.cch
  Opens:                  C:\Windows\System32\combase.dll
  Opens:                  C:\Windows\System32\shell32.dll
  Opens:                  C:\Windows\System32\SHCore.dll
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\System32\profapi.dll
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\64bit\security.config
  Opens:                  C:\Users\Admin\AppData\Roaming\Microsoft\CLR Security
Config\v2.0.50727.312\64bit\security.config.cch
  Opens:                  C:\Windows\assembly\NativeImages_v2.0.50727_64\index21.dat
  Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\da1374321aba580a5d2ec1c436b7f627\mscorlib.ni.dll
  Opens:                  C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089
  Opens:                  C:\Windows\Temp
  Opens:                  C:\Windows\System32\ole32.dll
  Opens:                  C:\Windows\System32\oleaut32.dll
  Opens:                  C:\Windows\System32\rpcss.dll
  Opens:                  C:\Windows\System32\cryptbase.dll
  Opens:                  C:\Windows\System32\bcryptprimitives.dll
  Opens:                  C:\Windows\System32\uxtheme.dll
  Opens:                  C:\Windows\System32\l_intl.nls
  Opens:                  C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorjit.dll
  Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\5a205dcf58af0d8e6bf8a3cf6ca71f2d\System.ni.dll
  Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\2a97d798d61ed181a3219f67584767c5\System.Drawing.ni.dll
  Opens:
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\32f33718184def7f38864ecfd4b96114\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\System.Windows.Forms.dll
  Opens:                  C:\Windows\System32\dwmapi.dll
  Opens:
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_72771d4ecc1c3a4d
  Opens:
C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.9200.16384_none_72771d4ecc1c3a4d\GdiPlus.dll
  Opens:                  C:\Windows\System32\DWrite.dll
  Opens:                  C:\Windows\Fonts\micross.ttf
  Opens:                  C:\Windows\System32\en-US\user32.dll.mui
  Opens:                  C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
  Opens:                  C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
  Opens:                  C:\Windows\WindowsShell.Manifest
  Opens:                  C:\Windows\system32\uxtheme.dll.Config
  Opens:                  C:\Windows\System32\cmd.exe
  Opens:                  C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Opens:                  C:
  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\wbem
  Opens:                  C:\Windows\System32\wbem\WMIC.exe
  Opens:                  C:\Windows\System32\locale.nls
  Opens:                  C:\Windows\System32\winbrand.dll
  Opens:                  C:\Windows\Branding\Basebrd\basebrd.dll
  Opens:                  C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
  Opens:                  C:\Windows\System32\en-US\cmd.exe.mui
  Opens:                  C:\Windows\System32\conhost.exe
  Opens:                  C:\Windows\System32\en-US\conhost.exe.mui
  Opens:                  C:\Windows\System32\cryptsp.dll
  Opens:                  C:\Windows\System32\rsaenh.dll
  Opens:                  C:\Windows\System32\nslookup.exe
  Opens:                  C:\Windows\Prefetch\NSLOOKUP.EXE-3D06E09F.pf
  Opens:                  C:\Windows\System32\wsock32.dll
  Opens:                  C:\Windows\System32\dnsapi.dll
  Opens:                  C:\Windows\System32\mswsock.dll
  Opens:                  C:\Windows\System32\nsi.dll
  Opens:                  C:\Windows\System32\ws2_32.dll
  Opens:                  C:\Windows\System32\en-US\nslookup.exe.mui
  Opens:                  C:\Windows\System32\NapiNSP.dll
  Opens:                  C:\Windows\System32\pnrpnsp.dll
  Opens:                  C:\Windows\System32\nlaapi.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
  Opens:                  C:\Windows\Fonts\StaticCache.dat
  Opens:                  C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
  Opens:
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
  Reads from:             C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
  Reads from:             C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Reads from:             C:\Windows\Fonts\StaticCache.dat
```

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
  Receives data from:     8.8.8.8:53
```

Windows Registry Events

```
  Creates key:            HKLM\software\microsoft\fusion\gacchangenotification\default
  Creates key:            HKLM\system\currentcontrolset\services\tcpip\parameters
  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\system\currentcontrolset\control\session manager
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:              HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:              HKLM\
  Opens key:              HKLM\software\microsoft\.netframework\policy\
  Opens key:              HKLM\software\microsoft\.netframework\policy\v4.0
  Opens key:              HKLM\software\microsoft\.netframework
  Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:              HKLM\software\microsoft\sqmclient\windows
  Opens key:              HKCU\software\microsoft\.netframework
  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\.netframework\policy\standards
  Opens key:              HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
  Opens key:              HKLM\software\microsoft\fusion
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\software\microsoft\.netframework\policy\apppatch
  Opens key:              HKLM\software\microsoft\.netframework\policy\apppatch\v4.0.30319.00000
  Opens key:
HKLM\software\microsoft\.netframework\policy\apppatch\v4.0.30319.00000\mscorwks.dll
  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\ngen\policy\v2.0
  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-
1923240461-1905901954-2556564120-1001
  Opens key:              HKLM\software\microsoft\ole
  Opens key:              HKLM\software\microsoft\ole\tracing
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions
  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\system\currentcontrolset\control\nls\sorting\ids
  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_64
  Opens key:                HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\index21
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  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_64\ni\38c56119\1d3ee2d7
  Opens key:                HKLM\software\microsoft\strongname
  Opens key:                HKLM\software\microsoft\.netframework\internal\jit\perf
  Opens key:                HKLM\software\microsoft\fusion\publisherpolicy\default
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9
  Opens key:                HKLM\software\microsoft\.netframework\policy\aptca
  Opens key:                HKLM\hardware\devicemap\video
  Opens key:                HKLM\system\currentcontrolset\control\video\{bf735b18-1b5a-4e14-b64c-
f2223c917d28}\0000
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
  Opens key:                HKLM\system\currentcontrolset\services\fontcache\parameters
  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\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:               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\image file execution
options\conhost.exe
  Opens key:               HKLM\software\microsoft\oleaut
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
  Opens key:               HKCU\console
  Opens key:               HKCU\console\
  Opens key:               HKLM\software\microsoft\rpc
  Opens key:               HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:               HKCU\console\%systemroot%_system32_cmd.exe
  Opens key:               HKCU\console\%systemroot%\system32\cmd.exe
  Opens key:               HKLM\system\setup
  Opens key:               HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:               HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
  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\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  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\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:               HKLM\software\microsoft\windows\windows error reporting\wmr
  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\software\microsoft\windows nt\currentversion\image file execution
options\nslookup.exe
  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\00000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
```

```
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
   Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
   Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
   Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
   Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
   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\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
   Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a04231f6-42eb-4732-b850-
25b8d56dd1d8}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{4defd920-8095-41dc-aef5-
8a6dc56e0da9}
   Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}
   Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
   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\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\
   Opens key:                HKLM\software\rajivapp1\rajivapp1\1.0.0.0
   Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
   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\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:            HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
   Queries value:            HKLM\software\microsoft\.netframework[installroot]
   Queries value:            HKLM\software\microsoft\.netframework[clrloadlogdir]
   Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
   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[uselegacyv2runtimeactivationpolicydefaultvalue]
   Queries value:            HKLM\software\microsoft\.netframework[onlyuselatestclr]
   Queries value:            HKLM\software\microsoft\fusion[noclientchecks]
   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\windows nt\currentversion\image file execution
options[devoverrideenable]
  Queries value:
HKLM\software\microsoft\.netframework\ngen\policy\v2.0[optimizeusedbinaries]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  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\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  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-
1923240461-1905901954-2556564120-1001[profileimagepath]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64[latestindex]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\index21[niusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\index21[ilusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\181938c6\7950e2c5\1[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\7950e2c5\6f33d37e\1[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,amd64]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
```

```
   Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
   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\.netframework[cseon]
   Queries value:            HKLM\software\microsoft\.netframework[tailcallopt]
   Queries value:            HKLM\software\microsoft\.netframework[pinvokeinline]
   Queries value:            HKLM\software\microsoft\.netframework[pinvokecalliopt]
   Queries value:            HKLM\software\microsoft\.netframework[newgccalc]
   Queries value:            HKLM\software\microsoft\.netframework[turnoffdebuginfo]
   Queries value:            HKLM\software\microsoft\.netframework[disablehotcold]
   Queries value:            HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[nidependencies]
   Queries value:
```

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\61e7e666\c991064\10[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\475dce40\6604efc\3[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\19ab8d57\5206cfdb\7[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\2dd6ac50\6bbd663d\4[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\424bd4d8\210819fb\6[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\41c04c7e\7a981124\1f[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3ced59c5\bd38540\f[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\c991064\34e16fb6\20[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[nidependencies]
  Queries value:
```

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\30bc7c4f\3f50fe4f\8[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\3f50fe4f\6ff8cf57\8[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\ni\3cca06a0\6dc7d4c0\9[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_64\il\6dc7d4c0\153b7f91\9[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\video0]
   Queries value:              HKLM\system\currentcontrolset\control\class\{4d36e968-e325-11ce-bfc1-
08002be10318}\0000[pruningmode]
   Queries value:
HKLM\system\currentcontrolset\services\fontcache\parameters[clientcachesize]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ko-kr]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ko-kr]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-tw]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw]
   Queries value:              HKLM\system\currentcontrolset\control\nls\customlocale[zh-hk]
   Queries value:              HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hk]
   Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
   Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
   Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
   Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
   Queries value:              HKCU\console[screencolors]
   Queries value:              HKCU\console[popupcolors]
```

```
  Queries value:            HKCU\console[insertmode]
  Queries value:            HKCU\console[quickedit]
  Queries value:            HKCU\console[codepage]
  Queries value:            HKCU\console[screenbuffersize]
  Queries value:            HKCU\console[windowsize]
  Queries value:            HKCU\console[windowposition]
  Queries value:            HKCU\console[fontsize]
  Queries value:            HKCU\console[fontfamily]
  Queries value:            HKCU\console[fontweight]
  Queries value:            HKCU\console[facename]
  Queries value:            HKCU\console[cursorsize]
  Queries value:            HKCU\console[historybuffersize]
  Queries value:            HKCU\console[numberofhistorybuffers]
  Queries value:            HKCU\console[historynodup]
  Queries value:            HKCU\console[colortable00]
  Queries value:            HKCU\console[colortable01]
  Queries value:            HKCU\console[colortable02]
  Queries value:            HKCU\console[colortable03]
  Queries value:            HKCU\console[colortable04]
  Queries value:            HKCU\console[colortable05]
  Queries value:            HKCU\console[colortable06]
  Queries value:            HKCU\console[colortable07]
  Queries value:            HKCU\console[colortable08]
  Queries value:            HKCU\console[colortable09]
  Queries value:            HKCU\console[colortable10]
  Queries value:            HKCU\console[colortable11]
  Queries value:            HKCU\console[colortable12]
  Queries value:            HKCU\console[colortable13]
  Queries value:            HKCU\console[colortable14]
  Queries value:            HKCU\console[colortable15]
  Queries value:            HKCU\console[loadconime]
  Queries value:            HKCU\console[extendededitkey]
  Queries value:            HKCU\console[extendededitkeycustom]
  Queries value:            HKCU\console[worddelimiters]
  Queries value:            HKCU\console[trimleadingzeros]
  Queries value:            HKCU\console[enablecolorselection]
  Queries value:            HKCU\console[scrollscale]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\microsoft\rpc[idletimerwindow]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  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\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\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:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:            HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:            HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  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_entries64]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[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_entries64]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[supportednamespace]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[librarypath]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[displaystring]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[addressfamily]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[supportednamespace]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[enabled]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[storesserviceclassinfo]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\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\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[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[disablesmartnameresolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[preferlocaloverlowerbindingdns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[querynetbtfqdn]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disablesmartprotocolreordering]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[udprecvbuffersize]
   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[newdhcpsrvregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[directaccesspreferlocal]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[disableidnencoding]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[enableidnmapping]
   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\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enabledhcp]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpv6domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[dhcpnameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[dhcpnameserver]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[maxnumberofaddressestoregister]
   Queries value:
```

```
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b5105d63-74c6-4dc1-87b7-
55779daa70e9}[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{97e1de57-d6fa-11e1-be62-
806e6f6e6963}[enablemulticast]
  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\software\microsoft\ctf[enableanchorcontext]
```