

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 617, Task ID: 2414

Task ID:	2414
Risk Level:	5
Date Processed:	2016-02-22 05:27:17 (UTC)
Processing Time:	56.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe"
Sample ID:	617
Type:	basic
Owner:	admin
Label:	262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36
Date Added:	2016-02-22 05:26:48 (UTC)
File Type:	PE32:win32:gui
File Size:	41472 bytes
MD5:	0bf067750c7406cf3373525dd09c293c
SHA256:	262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36
Description:	None

Pattern Matching Results

5 Abnormal sleep detected

Process/Thread Events

Creates process:
C:\WINDOWS\Temp\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe
["c:\windows\temp\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe"]
Terminates process:
C:\WINDOWS\Temp\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe

Named Object Events

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens: C:\WINDOWS\Prefetch\262058EA75F3CE8C666977449791B-0AFDA414.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winmm.dll
Opens: C:\WINDOWS\system32\rtm.dll
Opens: C:\WINDOWS\system32\rtutils.dll
Opens: C:\WINDOWS\system32\wssock32.dll
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\clusapi.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\0Aq7UdfxpdJws8vWfAF
Opens: C:\WINDOWS\system32\cmdial32.dll
Opens: C:\WINDOWS\system32\cmpbk32.dll
Opens: C:\WINDOWS\system32\cmutil.dll
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\comctl32.dll
Opens: C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens: C:\WINDOWS\system32\comctl32.dll.124.Config
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\system32\winrnr.dll
Opens: C:\WINDOWS\system32\drivers\etc\hosts
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\WINDOWS\system32\rasadhlp.dll
Reads from: C:\WINDOWS\system32\drivers\etc\hosts
Reads from: C:\WINDOWS\system32\rsaenh.dll

Network Events

DNS query: guphumsa.ru

DNS query: wowrizep.ru
Sends data to: 8.8.8.8:53
Receives data from: 0.0.0.0:0

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\rpcrt4.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\advapi32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\winmm.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcrt.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtutils.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2help.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ws2_32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\wsock32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\rtm.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\oleaut32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\clusapi.dll
Opens key:	HKLM\system\currentcontrolset\control\error message instrument\
Opens key:	HKLM\system\currentcontrolset\control\error message instrument
Opens key:	HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key:	HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key:	HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows nt\currentversion\drivers32
Opens key:	HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKCR\interface
Opens key:	HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\oleaut\userera
Opens key:	HKCU\
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmutil.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\cmpbk32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key:	HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key:	HKLM\system\setup
Opens key:	

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comctl32.dll
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\cmdial32.dll
 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\000000004
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

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

options\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe\rpcthreadpoolthrottle
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\microsoft\rpc\securityservice
 Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

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

options\iphlpapi.dll
 Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
 Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\
 Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
 Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
 Opens key:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}
 Opens key: HKLM\software\policies\microsoft\system\dnsclient
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

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

options\winrnr.dll
 Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rsaenh.dll
 Opens key: HKLM\software\policies\microsoft\cryptography
 Opens key: HKLM\software\microsoft\cryptography
 Opens key: HKLM\software\microsoft\cryptography\offload
 Opens key: HKLM\system\currentcontrolset\control\wmi\security
 Opens key: HKLM\system\currentcontrolset\control\computername
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\rasadhlp.dll
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows

nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime

compatibility[262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
 Queries value:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
 Queries value: HKLM\system\currentcontrolset\control\session

manager[criticalsectiontimeout]
 Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
 Queries value: HKCR\interface[interfacehelperperdisableall]
 Queries value: HKCR\interface[interfacehelperperdisableallforole32]
 Queries value: HKCR\interface[interfacehelperperdisabletypelib]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperperdisableall]
 Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperperdisableallforole32]
 Queries value: HKCU\control panel\desktop[multiuilanguageid]
 Queries value: HKLM\system\setup[systemsetupinprogress]
 Queries value: HKCU\control panel\desktop[smoothscroll]
 Queries value:

HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
 Queries value:

[illegible]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[appendtomultilabelname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlDs]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usedns]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressesstoregister]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatezoneexcludefile]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[updatetopleveldomainzones]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]

Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxCachesize]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxCacheTtl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxNegativeCacheTtl]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[adapterTimeoutLimit]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[serverPriorityTimeLimit]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[maxCachedSockets]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastListenLevel]
Queries value:
HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastSendLevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsQueryTimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsQuickQueryTimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsMulticastQueryTimeouts]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseObtainedTime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseTerminateTime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpServer]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[queryAdapterName]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableAdapterDomainName]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationEnabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registerAdapterName]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationMaxAddressCount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxNumberOfAddressesToRegister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpDomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipAutoConfigurationEnabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addressType]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpNameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchList]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsBtLookupOrder]
Queries value: HKLM\system\currentcontrolset\services\ldap[ldapClientIntegrity]
Queries value: HKLM\software\microsoft\cryptology\defaults\provider\microsoft strong cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptology\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeProcessSearchMode]
Queries value: HKLM\software\microsoft\cryptology[machineGuid]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-

ab78-1084642581fb]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]

Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\currentcontrolset\services\netbt\linkage[export]

Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodiald11]

Value changes: HKLM\software\microsoft\cryptography\rng[seed]