

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 614, Task ID: 2404

Task ID:	2404
Risk Level:	5
Date Processed:	2016-02-22 05:26:52 (UTC)
Processing Time:	62.43 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe"
Sample ID:	614
Type:	basic
Owner:	admin
Label:	7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20
Date Added:	2016-02-22 05:26:48 (UTC)
File Type:	PE32:win32:gui
File Size:	55808 bytes
MD5:	093586512549f2d016ad4c70f4f8e5c8
SHA256:	7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20
Description:	None

Pattern Matching Results

- 5 Abnormal sleep detected
- 5 PE: Contains compressed section

Process/Thread Events

Creates process:
C:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe
["C:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \BaseNamedObjects\SvcctrlStartEvent_A3752DX

File System Events

Opens: C:\Windows\Prefetch\7A495357099319383D3E509A676B5-49B7ACAE.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\windows\temp\REGAPI.dll
Opens: C:\Windows\SysWOW64\regapi.dll
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\SQLUNIRL.dll
Opens: C:\Windows\SysWOW64\sqlunirl.dll
Opens: C:\windows\temp\WINSPPOOL.DRV
Opens: C:\Windows\SysWOW64\winspool.drv
Opens:
C:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\comdlg32.dll
Opens: C:\Windows\SysWOW64\nddeapi.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\windows\temp\cmDial32.dll
Opens: C:\Windows\SysWOW64\cmdial32.dll
Opens: C:\windows\temp\cmpbk32.dll
Opens: C:\Windows\SysWOW64\cmpbk32.dll
Opens: C:\windows\temp\cmutil.dll
Opens: C:\Windows\SysWOW64\cmutil.dll
Opens: C:\windows\temp\eappcfg.dll
Opens: C:\Windows\SysWOW64\eappcfg.dll
Opens: C:\windows\temp\USERENV.dll
Opens: C:\Windows\SysWOW64\userenv.dll
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\SysWOW64\profapi.dll

Opens:	C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens:	C:\windows\temp\wsock32.dll
Opens:	C:\Windows\SysWOW64\wsock32.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\mswsock.dll
Opens:	C:\Windows\SysWOW64\WSH_TCPIP.DLL
Opens:	C:\Windows\SysWOW64\nlaapi.dll
Opens:	C:\Windows\SysWOW64\NapiNSP.dll
Opens:	C:\Windows\SysWOW64\pnrpnp.dll
Opens:	C:\windows\temp\DNSAPI.dll
Opens:	C:\Windows\SysWOW64\dnsapi.dll
Opens:	C:\Windows\SysWOW64\winrnr.dll
Opens:	C:\windows\temp\IPHLPAPI.DLL
Opens:	C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:	C:\windows\temp\WINNSI.DLL
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\windows\temp\dhcpcsvc6.DLL
Opens:	C:\Windows\SysWOW64\dhcpcsvc6.dll
Opens:	C:\windows\temp\dhcpcsvc.DLL
Opens:	C:\Windows\SysWOW64\dhcpcsvc.dll
Opens:	C:\Windows\System32\drivers\etc\hosts
Opens:	C:\windows\temp\rasadhlp.dll
Opens:	C:\Windows\SysWOW64\rasadhlp.dll
Reads from:	C:\Windows\System32\drivers\etc\hosts

Network Events

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

Windows Registry Events

Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dl
Opens key:	
	HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\system\currentcontrolset\control\ls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\ls\language
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key:	HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key:	HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key:	HKLM\software\policies\microsoft\mui\settings
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
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\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key:	
	HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:	HKLM\system\currentcontrolset\control\ls\sorting\versions
Opens key:	HKLM\
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\gre_initialize
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime compatibility
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key:	HKCU\software\microsoft\microsoft sql server\80\tools\client
Opens key:	HKCU\software\microsoft\microsoft sql server\80\tools\sqlstr
Opens key:	HKLM\software\wow6432node\microsoft\ole
Opens key:	HKLM\software\wow6432node\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\wow6432node\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\control\cmf\config
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
 Opens key: HKLM\software\microsoft\windows\currentversion\setup
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
 Opens key: HKLM\software\policies\microsoft\sqlclient\windows
 Opens key: HKLM\software\microsoft\sqlclient\windows
 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\36c46158
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\000000005
 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\namespace_catalog5
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\000000028
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
 Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
 Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
 Opens key: HKLM\system\currentcontrolset\services\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\software\wow6432node\microsoft\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\setup
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
 Opens key: HKLM\software\wow6432node\policies\microsoft\system\dnsclient
 Opens key: HKLM\software\policies\microsoft\system\dnsclient
 Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key: HKLM\system\currentcontrolset\services\dnsclient\parameters\dnsclient
 Opens key: HKLM\system\currentcontrolset\services\dns
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\dnsclient\dnsclientpolicyconfig
 Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient\dnsclientpolicyconfig
 Opens key:
 HKLM\system\currentcontrolset\services\dnsclient\parameters\dnsclientpolicyconfig
 Opens key:
 HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}
Opens key:
HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{a91d0a5e-390e-4979-9c38-127795cce47a}
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{b9ec5865-2d36-4cb8-b474-65fee5bae0b1}
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\netbt\linkage
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\locale\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\locale\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatencodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\locale\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[sqlunirl.dll]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\system\currentcontrolset\control\locale\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\locale\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-b16d-46121d0255aa]
Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:

[illegible]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storiesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup\systemsetupinprogress
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value: HKLM\system\currentcontrolset\control\sqm\servicelist[sqm\servicelist]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters\dns\cache[shutdownonidle]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[domainnamedevolutionlevel]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value:
HKLM\system\currentcontrolset\services\dns\cache\parameters[appendtomultilabelname]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screenbadtlDs]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screenunreachableservers]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[screendefaultservers]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dynamicserverqueryorder]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[filterclusterip]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[useedns]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnssecurenamequeryfallback]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[enabledaforallnetworks]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[directaccessqueryorder]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[usehostsfile]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[addrconfigcontrol]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationenabled]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerprimaryname]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registeradaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerreverselookup]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registerwanadapters]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationttl]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationrefreshinterval]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationmaxaddresscount]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddresstoregister]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[updatesecuritylevel]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[updatetopleveldomainzones]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[downcasespncauseapiowneristoolazy]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[registrationoverwrite]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachettl]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxnegativecachettl]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[adaptertimeoutlimit]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[serverprioritytimelimit]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[maxcachedsockets]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[enablemulticast]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastresponderflags]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsenderflags]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[multicastsendermaxtimeout]
Queries value: HKLM\system\currentcontrolset\services\dnsCache\parameters[dnstest]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usecompartments]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[cacheallcompartments]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[usenewregistration]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistration]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[resolverregistrationonly]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\dnsCache\parameters[dnsquickquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[searchlist]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[enabledhcp]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationenabled]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registeradaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[domain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpdomain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpv6domain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[nameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[dhcpnameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enabledhcp]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationenabled]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registeradaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[domain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpdomain]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[nameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[dhcpnameserver]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[queryadaptername]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[disableadapterdomainname]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[registrationmaxaddresscount]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-e1e01c1f69b5}[maxnumberofaddressesstoregister]
Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{22873b3e-c4d3-495a-8165-


```
e1e01c1f69b5}[enablemulticast]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[maxnumberofaddresstoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{846ee342-7039-11de-9d20-806e6f6e6963}[enablemulticast]
  Queries value:      HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:      HKLM\system\currentcontrolset\services\netbt\linkage[export]
  Queries value:      HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
```