# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 629, Task ID: 2464

Task ID: 2464 Risk Level: 5

Risk Level: 5

Date Processed: 2016-02-22 05:32:58 (UTC)

Processing Time: 65.3 seconds
Virtual Environment: IntelliVM

**Execution Arguments:** 

c:\windows\temp\aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1.exe"

Sample ID: 629 Type: basic Owner: admin

Label: aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1

Date Added: 2016-02-22 05:26:50 (UTC)

File Type: PE32:win32:gui File Size: 43520 bytes

MD5: 08862142d7313a1d431d67e0e755efc7

SHA256: aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1

Description: None

## Pattern Matching Results

5 Abnormal sleep detected

5 PE: Contains compressed section

#### Process/Thread Events

Creates process:

C:\windows\temp\aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1.exe ["C:\windows\temp\aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1.exe" ]

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \BaseNamedObjects\SvcctrlStartEvent\_A3752DX

#### File System Events

Opens:	C:\Windows\Prefetch\AA9F8C1C8818B356427331F5A3F20-2115DB4F.pf
--------	---

Opens: C:\Windows

 Opens:
 C:\Windows\System32\wow64.dl1

 Opens:
 C:\Windows\System32\wow64win.dl1

 Opens:
 C:\Windows\System32\wow64cpu.dl1

 Opens:
 C:\Windows\system32\wow64log.dl1

Opens: C:\Windows\SysWOW64

C:\windows\temp\CERTCLI.dll Opens: Opens: C:\Windows\SysWOW64\certcli.dll Opens: C:\windows\temp\ATL.DLL C:\Windows\SysWOW64\atl.dll Opens: Opens: C:\Windows\SysWOW64\sechost.dll Opens: C:\windows\temp\SQLUNIRL.dll C:\Windows\SysWOW64\sqlunirl.dll Opens: Opens: C:\windows\temp\WINSPOOL.DRV Opens: C:\Windows\SysWOW64\winspool.drv

Opens:

C:\windows\temp\aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1.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\Globalization\Sorting\SortDefault.nls

Opens: C:\Windows\SysWOW64\comdlg32.dll Opens: C:\Windows\SysWOW64\nddeapi.dll Opens: C:\Windows\SysWOW64\shell32.dll Opens: C:\Windows\SysWOW64\kernel32.dll C:\Windows\SysWOW64\gdi32.dll Opens: Opens: C:\Windows\SysWOW64\advapi32.dll C:\Windows\SysWOW64\user32.dll Opens: Opens: C:\windows\temp\cmDIAl32.dll Opens: C:\Windows\SysWOW64\cmdial32.dll Opens: C:\windows\temp\cmpbk32.dll C:\Windows\SvsWOW64\cmpbk32.dll Opens: Opens: C:\windows\temp\cmutil.dll C:\Windows\SysWOW64\cmutil.dll Opens: Opens: C:\windows\temp\eappcfg.dll

Opens: C:\Windows\SysWOW64\eappcfg.dll
Opens: C:\windows\temp\USERENV.dll

Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui

Opens: C:\windows\temp\wsock32.dll C:\Windows\SysWOW64\wsock32.dll Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\WSHTCPIP.DLL Opens: Opens: C:\Windows\SysWOW64\nlaapi.dll C:\Windows\SysWOW64\NapiNSP.dll Opens: Opens: C:\Windows\SysWOW64\pnrpnsp.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 C:\Windows\SysWOW64\IPHLPAPI.DLL Opens: Opens: C:\windows\temp\WINNSI.DLL Opens: C:\Windows\SysWOW64\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\SysWOW64\dhcpcsvc.dll
Opens: C:\Windows\System32\drivers\etc\hosts

#### **Network Events**

DNS query: merwiqca.ru
DNS query: wowrizep.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\dll
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\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\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:

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\diagnostics

 $Opens\ key: \\ HKLM\ software\ microsoft\ windows\ nt\ current version\ image\ file\ execution$ 

options\dllnxoptions

Opens key: HKLM\software\wow6432node\microsoft\windows

 $\verb|nt\current| version \verb|\gre_initialize| \\$ 

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: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\system\currentcontrolset\services\ldap

Opens key: HKCU\software\microsoft\microsoft sql server\80\tools\client
Opens key: HKCU\software\microsoft\microsoft sql server\80\tools\sqlstr

```
\label{lem:hklm} \verb+Kklm \+ system \+ control \+ ls \+ extended locale
 Opens key:
 Opens key:
                     HKLM\software\wow6432node\microsoft\ole
 Opens kev:
                     HKLM\software\wow6432node\microsoft\ole\tracing
                     HKLM\software\microsoft\ole\tracing
 Opens key:
 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
                     HKLM\software\wow6432node\microsoft\windows\currentversion\setup
 Opens key:
 Opens key:
                     HKLM\software\microsoft\windows\currentversion\setup
 Opens key:
                     HKLM\software\wow6432node\microsoft\windows\currentversion
                     HKLM\software\policies\microsoft\samclient\windows
 Opens key:
 Opens key:
                     HKLM\software\microsoft\sqmclient\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\34ef9163
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9 \setminus 00000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001
 Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens kev:
Opens kev:
Opens kev:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
 Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001
 Opens kev:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
 Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000006
 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:
                     {\tt HKLM \ } system \verb|\ current control \ \\ computer name \verb|\ active computer name \ \\ 
 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\dnscache\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 kev:
                     HKLM\software\policies\microsoft\system\dnsclient
 Opens key:
                     HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key:
                     HKLM\system\currentcontrolset\services\dnscache\parameters\dnscache
 Opens key:
                     HKLM\system\currentcontrolset\services\dns
 Opens key:
                     HKLM\software\wow6432node\policies\microsoft\windows
nt\dnsclient\dnspolicyconfig
                     HKLM\software\policies\microsoft\windows nt\dnsclient\dnspolicyconfig
 Opens key:
 Opens key:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters\dnspolicyconfig
   Opens kev:
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
   Oueries 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]
   Oueries value:
HKLM \ software \ policies \ microsoft \ windows \ safer \ code identifiers \ [transparentenabled]
   Queries value:
                                                HKLM\system\currentcontrolset\control\nls\customlocale[empty]
   Queries value:
HKLM \verb|\system| current control \verb|\system| current control \verb|\system| control \verb|\system| current control current control current control current control current control current control current current control current current control current current current current control current current
   Queries value:
                                                 HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
                                                 HKLM\system\currentcontrolset\control\mui\uilanguages\en-
   Oueries value:
us[alternatecodepage]
   Queries value:
                                                 HKCU\control panel\desktop[preferreduilanguages]
                                                 \label{lem:hkcu} \verb|HKCU| control panel| desktop| \verb|muicached[machinepreferreduil] anguages]| \\
   Oueries value:
   Queries value:
HKLM \setminus software \setminus wow6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side [prefer external manifest]
   Oueries value:
                                                 HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                                 HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
   Queries value:
   Queries value:
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
                                                 HKLM\software\microsoft\windows nt\currentversion\image file execution
   Oueries value:
options\dllnxoptions[sqlunirl.dll]
   Oueries value:
                                                 HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                                HKLM\software\wow6432node\microsoft\windows
   Oueries value:
nt \verb|\currentversion| compatibility 32[aa9f8c1c8818b356427331f5a3f208f683ee750ddb34cd480587584c11e98fc1]| and the substitution of the substituti
                                                HKLM\software\wow6432node\microsoft\windows
   Oueries value:
nt\currentversion\windows[loadappinit dlls]
   Oueries value:
                                                 HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
                                                 HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
   Queries value:
   Oueries value:
                                                 HKLM\svstem\currentcontrolset\services\ldap[useoldhostresolutionorder]
   Queries value:
                                                 HKLM\system\currentcontrolset\services\ldap[usehostnameasalias]
                                                 HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
   Oueries value:
   Queries value:
                                                 HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
   Oueries value:
                                                 HKLM\software\microsoft\ole[pageallocatorusesystemheap]
   Queries value:
                                                 HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\cmf\config[system]
   Oueries value:
                                                 HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
   Oueries value:
                                                 HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
                                                 HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   Queries value:
                                                 HKLM\system\currentcontrolset\control\wmi\security[5f31090b-d990-4e91-
   Oueries value:
b16d-46121d0255aa]
   Oueries value:
                                                 HKLM\software\microsoft\sqmclient\windows[ceipenable]
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
   Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
   Oueries 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]
   Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 000000000001 \ [packed catalog item]
   Queries value:
```

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ 00000000000002 \ [packed catalog item] \\ Queries \ value:$ 

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003[packedcatalogitem] Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000006[packedcatalogitem]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000007[packedcatalogitem]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000009[packedcatalogitem]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[serial\_access\_num]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5[num\_catalog\_entries]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[supportednamespace]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[enabled]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[storesserviceclassinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[providerinfo]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[displaystring]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerid]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[addressfamily]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[supportednamespace]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[version]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 00000000000002 [provider info] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[librarypath]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[displaystring]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[version]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[librarypath]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[providerid]
   Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[addressfamily]
  Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace\_catalog 5 \setminus catalog\_entries \setminus 0000000000004 [enabled]$ 

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000004[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerinfo]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[displaystring]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerid]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[addressfamily]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[version]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerinfo]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[librarypath]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[displaystring] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ winsock 2 \ parameters \ name \ space\_catalog \ services \ name \ space\_catalog \ name \ name \ name \ space\_catalog \ name \$ 

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000006[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[enabled]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[version]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[storesserviceclassinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[providerinfo]
 Oueries 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]

 $\label{thm:prop:prop:prop:queries} Queries value: & HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] \\$ 

Queries value: HKLM\system\currentcontrolset\services\winsock\setup migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]$ 

Queries value:

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]

Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Oueries value:

HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]

Oueries 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\sqmservicelist[sqmservicelist]

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
 Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
 Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[domainnamedevolutionlevel]
 Oueries value:

 $\label{lem:hklmsystem} HKLM \ system \ current controls et \ services \ dns cache \ parameters \ [prioritize record data] \\ Queries \ value:$ 

```
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Oueries 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]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screendefaultservers]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dynamicserverqueryorder]
   Queries value:
HKLM\svstem\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Oueries value:
                                               HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[dnssecurenamequeryfallback]
   Oueries 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]
                                               Oueries value:
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[addrconfigcontrol]
   Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [registration enabled]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Oueries value:
\label{thm:local_hammeters} \begin{tabular}{ll} HKLM \end{tabular} system \current control set \end{tabular} set \end{tabular} and \end{tabular} are the label \end{tabular} are the label \end{tabular} set \end{tabular} are the label \end{tabular} are the label \end{tabular} are the label \end{tabular} set \end{tabular} are the label \end{tabular} are the label \end{tabular} are the label \end{tabular} are the label \end{tabular} set \end{tabular} are the label \end{tabula
   Queries value:
HKLM \verb| system| current control set \verb| services| tcpip| parameters[enable adapter domain name registration]| to the system of 
HKLM\svstem\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Oueries 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]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Oueries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[downcasespncauseapiowneristoolazy]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationoverwrite]
                                                HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Oueries value:
                                                HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Oueries value:
   Queries value:
Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Oueries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Oueries value:
HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [enable multicast]
```

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[multicastresponderflags]

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsenderflags]

Oueries value:

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

Oueries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[usecompartments]

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [cacheall compartments]$ 

Queries value:

 $\label{thm:local-control} \begin{tabular}{ll} HKLM \end{tabular} is supported by the control of the control o$ 

Queries value:

Queries value:

Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[dnsquerytimeouts]

Queries value:

 ${\tt HKLM \ } system \verb| current control set \verb| services \verb| tcpip \verb| parameters [dns query time outs]|$ 

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:

 $\label{lem:hklm} HKLM \ system \ `current controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration enabled]$ 

Oueries value:

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

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [domain]$ 

Oueries 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:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [names erver]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [dhcpnames erver]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \end{20-806e6f6e6963} \ [enabled \hcp]$ 

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:

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \interfaces \end{20-806e6f6e6963} \ [dhcpnameserver]$ 

Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [queryadaptername]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [disable adapter domain name]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [registration maxaddress count]$ 

Oueries value

 $\label{lem:hklm} HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [maxnumber of addresses to register]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{22873b3e-c4d3-495a-8165-e1e01c1f69b5\} \ [enable multicast]$ 

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \true \parameters \true \noinder \noinder$ 

Queries value:

 $HKLM \ system \ current controls et \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [disable adapter domain name]$ 

Oueries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d 20-806e 6f 6e 6963\} \ [disable dynamic update]$ 

Queries value:

 $HKLM \ system \ `current control set \ 's ervices \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d 20-806e6 f 6e 6963\} \ [enable adapter domain name registration]$ 

Oueries value

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d 20-806e 6f 6e 6963\} \ [registration max address count]$ 

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [maxnumber of addresses to register]$ 

Queries value:

 $HKLM \ system \ `current control set \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{846ee 342-7039-11de-9d20-806e6f6e6963\} \ [enable multicast]$ 

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value: HKLM\system\currentcontrolset\services\netb\linkage[export]

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