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 C:\WINDOWS\system32\rtutils.dll Opens: Opens: C:\WINDOWS\system32\wsock32.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 C: 0Aq7UdfxpdJws8vWFaF Opens: Opens: C:\WINDOWS\system32\cmdial32.dll Opens: C:\WINDOWS\system32\cmpbk32.dll C:\WINDOWS\system32\cmutil.dll Opens: Opens: C:\WINDOWS\system32\shell32.dll Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest C:\WINDOWS\system32\SHELL32.dll.124.Config Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Opens: Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Opens: Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll Opens: C:\WINDOWS\WindowsShell.Manifest C:\WINDOWS\WindowsShell.Config Opens: Opens: C:\WINDOWS\system32\comctl32.dll

Opens: C:\WINDOWS\system32\comct132.d11
Opens: C:\WINDOWS\system32\comct132.d11.124.Manifest
Opens: C:\WINDOWS\system32\comct132.d11.124.Config
Opens: C:\WINDOWS\system32\windowsock.d11

Opens: C:\WINDOWS\system32\hnetcfg.dll Opens: C:\WINDOWS\system32\wshtcpip.dll Opens: C:\WINDOWS\system32\dnsapi.dll C:\WINDOWS\system32\iphlpapi.dll Opens: Opens: C:\WINDOWS\system32\winrnr.dll C:\WINDOWS\system32\drivers\etc\hosts Opens: Opens: C:\WINDOWS\system32\rsaenh.dll Opens: C:\WINDOWS\system32\crypt32.dll Opens: C:\WINDOWS\system32\rasadhlp.dll Reads from: C:\WINDOWS\svstem32\drivers\etc\hosts Reads from: C:\WINDOWS\system32\rsaenh.dll

Network Events

DNS query:

DNS query: wowrizep.ru 8.8.8.8:53 Sends data to: 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: ${\it HKLM \ } system \verb|\ current control \ safe boot \verb|\ option| \\$

Opens kev: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

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

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:

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 kev:

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

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

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

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:

options\clusapi.dll HKLM\system\currentcontrolset\control\error message instrument\ Opens key:

Opens key: HKLM\system\currentcontrolset\control\error message instrument Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize Opens kev: HKLM\software\microsoft\windows nt\currentversion\compatibilitv32 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-c000-00000000046}

HKLM\software\microsoft\oleaut Opens key: Opens key: HKLM\software\microsoft\oleaut\userera

Opens key: HKCU\

Opens key: HKCU\software\policies\microsoft\control panel\desktop

HKCU\control panel\desktop Opens key:

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

options\version.dll

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

options\cmutil.dll

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

options\cmpbk32.dll

Opens kev: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shlwapi.dll

HKLM\software\microsoft\windows\currentversion\explorer\performance Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shell32.dll

Opens key: HKLM\system\setup

Opens kev:

HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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 HKLM\system\currentcontrolset\services\winsock2\parameters Opens key: Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key: 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: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008 Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens kev: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5 HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000003 HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: 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 kev: HKLM\software\microsoft\windows nt\currentversion\image file execution options\262058ea75f3ce8c666977449791bbff87096144de755e38e63872de744eae36.exe\rpcthreadpoolthrottle HKLM\software\policies\microsoft\windows nt\rpc Opens key: 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: ${\it HKLM \ } system \ `current control set \ `services \ 'dn scache \ 'parameters$ Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\iphlpapi.dll Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage HKLM\system\currentcontrolset\services\tcpip\parameters\ Opens key: Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces HKLM\system\currentcontrolset\services\netbt\parameters Opens key: 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\wldap32.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 kev: 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\currentcontrol\set\control\wmi\security
Opens key: HKLM\system\currentcontrol\set\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]

Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave31 Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5] Oueries 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] Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]

HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8] HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4] HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6] Oueries value: Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7] Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]

Queries value:

HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer] Oueries 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] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5] Queries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6] Oueries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7] HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8] Oueries value: 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[interfacehelperdisableall]

Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableall]

Queries value: HKCR\interface\{00020400-0000-0000-c000-

00000000046}[interfacehelperdisableallforole32]

Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\control panel\desktop[smoothscroll]

Oueries value:

 $\label{thm:local_explorer} \begin{tabular}{ll} HKCU \software \verb|\microsoft| windows \verb|\currentversion| explorer \advanced[enableballoontips] \end{tabular}$

Queries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries 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\000000000004[packedcatalogitem]

 Oueries 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
 Queries value:
 HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
- $Queries\ value: \\ HKLM\ system\ current control set\ services\ winsock 2\ parameters\ protocol_catalog 9\ catalog_entries\ 000000000010[packed catalog item]$
- Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011[packedcatalogitem]
- Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- $HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000001 \ [providerid] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
- 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]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 numhandle buckets]$

Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2 32spincount] Oueries value: HKLM\software\microsoft\rpc[maxrpcsize] HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution] Oueries 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] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip] HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns] HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile] HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations] Oueries 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: $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [default registration ttl]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel] Oueries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]

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

Queries value:

Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize] Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachett1]

Oueries value:

Queries value:

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

Queries value:

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

Queries value:

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus dns cache \setminus parameters [multicast listen level]$

Oueries value:

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

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters [dnsquery time outs]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]

Oueries value:

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

Queries value:

 $HKLM \ system \ current controls et \ ervices \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [enabled \ hcp]$

Queries value:

 $HKLM \ system \ `controlset \ 'services \ 'tcpip \ parameters \ 'interfaces \ '\{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease obtained time]$

Queries value:

 $HKLM \ system \ current control set \ services \ trip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [lease terminates time]$

Oueries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} [dhcpserver]$

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

 $\label{local-hkl} $HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}\ [queryadaptername]$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]

Queries value:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \tcpip \parameters \interfaces \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} [registration enabled]$

Oueries value:

 $\label{lem:hklmsystem} HKLM \system \current control set \services \tcpip \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [register adapter name]$

Queries value:

 $HKLM \ system \ `correct Services \ 'tcpip \ parameters \ 'interfaces \ '\{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [registration maxaddress count]$

Queries value:

 $HKLM \ system \ current control set \ services \ tcpip \ parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [maxnumber of addresses to register]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \critector \crite$

Queries value:

 $\label{lem:hkkm} HKLM \system \current controls et \ervices \true \parameters \ interfaces \ \{16325b0b-4636-4303-abe3-c7d49d7cecdc\} \ [dhcpdomain]$

Queries value:

 $\label{lem:hklmsystem} HKLM \system \critical limits and the substitution of the sub$

Oueries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]

Queries value:

 $HKLM \simeq \frac{16325b0b-4636-4303-abe3-c7d49d7cecdc}{nameserver}$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]

 $\label{thm:current} Queries \ value: \\ HKLM \ system \ current control set \ services \ tcpip \ parameters \ [search list]$

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]

Queries value: HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider[type]

Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider[image path]

Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

Queries value: HKLM\software\microsoft\cryptography[machineguid]

Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-

ab78-1084642581fb]

0000-000000000000000000

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[autodialdl1]

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