# Malware Analysis Appliance by Blue Coat Systems, Inc.

#### Task Details

Host: mag2, Sample ID: 48, Task ID: 192

Task ID: 192 Risk Level: 1

Date Processed: 2016-04-28 12:52:23 (UTC)

Processing Time: 61.1 seconds
Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe"

Sample ID: 48
Type: basic
Owner: admin

Label: 9d240291c8dc756bfafe75a7e60099cc

Date Added: 2016-04-28 12:44:54 (UTC)
File Type: PE32:win32:gui

File Type: PE32:win32:gui File Size: 321536 bytes

MD5: 9d240291c8dc756bfafe75a7e60099cc

SHA256: 7c7b5307cc803bb037226eee0eca8b0a6f1d79d3d9d96755b29208442847466a

Description: None

## Pattern Matching Results

#### Static Events

Anomaly: PE: Contains a virtual section

### Process/Thread Events

Creates process: C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe

["C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe"]

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

## File System Events

Opens: C:\Windows\Prefetch\9D240291C8DC756BFAFE75A7E6009-B6910FBA.pf

Opens: C:\Windows

Opens: C:\Windows\SysWOW64

Opens: C:\Windows\SysWOW64\sechost.dll

Opens: C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe.Local\

Opens: C:\Windows\winsxs\x86\_microsoft.windows.common-

controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af

 $Opens: C: \windows \winsxs \x 86\_microsoft.windows.common-controls\_6595b64144ccf1df\_5.82.7601.17514\_none\_ec83dffa859149af\comctl32.dll$ 

Opens: C:\windows\temp\wsock32.dl1
Opens: C:\Windows\SysWOW64\wsock32.dl1
Opens: C:\Windows\SysWOW64\apphelp.dl1
Opens: C:\Windows\AppPatch\sysmain.sdb

Opens: C:\Windows\Temp\9d240291c8dc756bfafe75a7e60099cc.exe

C:\Windows\AppPatch\AcGenral.dll Opens: Opens: C:\windows\temp\UxTheme.dll Opens: C:\Windows\SysWOW64\uxtheme.dll Opens: C:\windows\temp\WINMM.dll Opens: C:\Windows\SysWOW64\winmm.dll Opens: C:\windows\temp\samcli.dll C:\Windows\SysWOW64\samcli.dll Opens: Opens: C:\windows\temp\MSACM32.dll Opens: C:\Windows\SysWOW64\msacm32.dll Opens: C:\windows\temp\VERSION.dll Opens: C:\Windows\SysWOW64\version.dll Opens: C:\windows\temp\sfc.dll C:\Windows\SysWOW64\sfc.dll Opens:

Opens: C:\windows\temp\sfc\_os.DLL C:\Windows\SysWOW64\sfc\_os.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\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll Opens: C:\windows\temp\MPR.dll Opens:

C:\Windows\SysWOW64\mpr.dll Opens:

Opens: C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe.Manifest

C:\Windows\SysWOW64\imm32.dll Opens:

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

Opens: C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.ENU Opens: C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.ENU.DLL Opens: C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.EN C:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.EN.DLL Opens: Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui

Opens: C:\Windows\Fonts\sserife.fon

Opens: C:\Windows\SysWOW64\UxTheme.dll.Config

C:\Windows\winsxs\x86\_microsoft.windows.common-Opens:

controls\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2

Opens: C:\Windows\winsxs\x86\_microsoft.windows.commoncontrols\_6595b64144ccf1df\_6.0.7601.17514\_none\_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\WindowsShell.Manifest Opens: C:\windows\temp\updatewizard.ini C:\Windows\SysWOW64\ole32.dll Opens: Opens: C:\Windows\SysWOW64\rpcss.dll Reads from: C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

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: 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 kev: HKLM\system\currentcontrolset\control\nls\customlocale

Opens key: HKLM\system\currentcontrolset\control\nls\language HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: 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 kev: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration  $HKLM \verb|\system| current controlset| control \verb|\mui| settings \verb|\language| configuration$ Opens key:

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

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

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags Opens kev: HKLM\svstem\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file

protection

HKLM\software\policies\microsoft\windows nt\windows file protection Opens key:

Opens key: HKLM\

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

nt\currentversion\diagnostics

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

nt\currentversion\gre\_initialize

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

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\software\wow6432node\microsoft\ole HKLM\software\wow6432node\microsoft\ole\tracing Opens key: Opens key: HKLM\software\microsoft\ole\tracing

Opens key: HKLM\software\wow6432node\microsoft\oleaut Opens key: HKLM\system\currentcontrolset\control\cmf\config

HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr Opens key: Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup

HKLM\software\microsoft\windows\currentversion\setup Opens key:

Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale

Opens key:  $HKLM \setminus system \setminus current control set \setminus services \setminus crypt 32$ 

Opens key:  $HKLM \ software \ wow 6432 node \ microsoft \ windows \ current version \ internet$ 

settings

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings

Opens kev: HKLM\software\policies\microsoft\windows\currentversion\internet

settings

Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder

Opens key: HKCU\software\borland\delphi\locales

Opens key: HKLM\system\currentcontrolset\control\nls\locale

HKLM\system\currentcontrolset\control\nls\locale\alternate sorts Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink

HKLM\software\microsoft\windows Opens kev:

 $\verb|nt\currentversion\languagepack\datastore\_v1.0|$ 

Opens key: HKLM\software\microsoft\windows

 $\verb|nt\current| version \verb|\language| pack \verb|\surrogatefall| back |$ 

Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui

Opens kev: HKLM\software\policies\microsoft\samclient\windows

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

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

HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid\_catalog\1ab01ca8

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries Opens kev:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ (catalog\_entries \ 0000000000001) \ (catalog\_entries \ (catalog\_entri$ Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000003 Opens kev:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\0000000000006 Opens key:

Opens kev:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000000 Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\00000028

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries 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 key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005 Opens key:

HKLM\software\microsoft\windows Opens key:

nt\currentversion\languagepack\surrogatefallback\ms sans serif

Opens key:

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus ctf \setminus compatibility \setminus 9d240291 \\ c8dc756b \\ fafe75a7e60099 \\ cc. exemple to the first of the first$ 

 $HKLM \setminus software \setminus wow 6432 \\ node \setminus microsoft \setminus tip \setminus \{0000897b - 83df - 4b96 - be07 - be07 - be07 - be18 \\ node \mid be18 \\ nod$ Opens key:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436} HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-Opens kev:

Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

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

Opens kev: HKLM\software\wow6432node\microsoft\ctf\knownclasses

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[disableusermodecallbackfilter]

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

manager[cwdillegalindllsearch]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]

Queries value:

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                         HKCU\control panel\desktop[preferreduilanguages]
 Oueries value:
 Oueries value:
                         HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Oueries value:
Queries value:
                         HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
                         HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Oueries value:
 Queries value:
                         HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
 Queries value:
                         HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                         HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\compatibility32[9d240291c8dc756bfafe75a7e60099cc]
                         HKLM\software\wow6432node\microsoft\windows
 Queries value:
nt\currentversion\windows[loadappinit dlls]
 Queries value:
                         HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value:
                         HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                         HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
                         HKLM\software\wow6432node\microsoft\windows\windows error
 Queries value:
reporting\wmr[disable]
                         HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Oueries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
                         HKLM \verb|\system| current controlset \verb|\services| crypt 32 [debugheapflags]
 Queries value:
 Queries value:
                         HKLM\software\wow6432node\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                         HKLM\software\policies\microsoft\windows\currentversion\internet
 Queries value:
settings[security_hklm_only]
                         HKLM\system\currentcontrolset\control\nls\locale[00000409]
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value:
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\datastore_v1.0[disable]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
 Queries value:
                         HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane5]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
                         HKLM\software\microsoft\windows
 Queries value:
\verb|nt\currentversion\language| pack\surrogatefallback[plane9]|
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
                         HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane14]
 Oueries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
 Oueries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM \ system \ current controls et \ services \ winsock 2 \ parameters \ protocol\_catalog9[serial\_access\_num]
 Queries 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:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ 000000000001 \ [packed catalog item] \\ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\0000000000002[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\000000000005[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] 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\currentcontrolset\services\winsock2\parameters\protocol\_catalog9\catalog\_entries\000000000010[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\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[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]
  Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace\_catalog 5 \ catalog\_entries \ 000000000001 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000001[storesserviceclassinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000001[providerinfo]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[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\0000000000002[addressfamily]
   Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000002[supportednamespace]
   Oueries value:
- 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000002[providerinfo]
  Oueries 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\000000000003[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000003[addressfamily]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[supportednamespace]
  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\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000003[providerinfo]
  Oueries value:

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[displaystring]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\0000000000004[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[supportednamespace]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[enabled]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000004[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]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[providerid]
- 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] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[version] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000005[storesserviceclassinfo]

  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000005[providerinfo] Oueries 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\0000000000006[displaystring]
  Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[providerid]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[addressfamily]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\000000000006[supportednamespace]
   Oueries 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]
  Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace\_catalog5\catalog\_entries\00000000006[storesserviceclassinfo] Oueries value:
- $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \namespace\_catalog 5 \catalog\_entries \namespace\_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2\_32numhandlebuckets]
- Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
- $0 fb 58b 01c 4a 4 \} \\ language profile \\ 0 x 00000000 \\ \{0001bea 3-ed 56-48 3d-a 2e 2-a ea e 25577436\} [enable]$
- Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]