Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 133, Task ID: 533

Task ID: 533 Risk Level:

Date Processed: 2016-04-28 13:01:32 (UTC)

Processing Time: 62.43 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\2a66d04f3cc49ec97d27a2555c853aba.exe"

Sample ID: Type: basic admin Owner:

2a66d04f3cc49ec97d27a2555c853aba Label:

2016-04-28 12:45:04 (UTC) Date Added: PE32:win32:gui

File Type: File Size: 506184 bytes

2a66d04f3cc49ec97d27a2555c853aba MD5:

4de7d43ad2a702eae423c5dcbbc0306289d128f435c221dcd43775017689e14f SHA256:

Description: None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\2a66d04f3cc49ec97d27a2555c853aba.exe

["C:\windows\temp\2a66d04f3cc49ec97d27a2555c853aba.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates event: \Sessions\1\BaseNamedObjects\ProtectorPlusHTTPScanEvent

File System Events

Opens: C:\Windows\Prefetch\2A66D04F3CC49EC97D27A2555C853-63D94479.pf

Opens: C:\Windows

Opens: C:\Windows\System32\wow64.dll Opens: C:\Windows\System32\wow64win.dll Opens: C:\Windows\System32\wow64cpu.dll Opens: C:\Windows\system32\wow64log.dll

Opens: C:\Windows\SysWOW64

Opens: C:\windows\temp\WSOCK32.dll Opens: C:\Windows\SysWOW64\wsock32.dll Opens: C:\Windows\SysWOW64\sechost.dll

Opens: C:\windows\temp\2a66d04f3cc49ec97d27a2555c853aba.exe.Local\

C:\Windows\winsxs\x86_microsoft.windows.common-Opens:

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

C:\Windows\winsxs\x86_microsoft.windows.common-Opens: controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

C:\windows\temp\WINSPOOL.DRV Opens: C:\Windows\SysWOW64\winspool.drv C:\windows\temp\oledlg.dll Opens: Opens: C:\Windows\SysWOW64\oledlg.dll Opens: C:\windows\temp\OLEPRO32.DLL C:\Windows\SysWOW64\olepro32.dll Opens: Opens: C:\Windows\SysWOW64\imm32.dll Opens: C:\Windows\SysWOW64\uxtheme.dll C:\Windows\Fonts\sserife.fon Opens: Opens: C:\windows\temp\dwmapi.dll Opens: C:\Windows\SysWOW64\dwmapi.dll

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

Opens: C:\Windows\Fonts\StaticCache.dat C:\windows\temp\Cleandos.exe Opens:

C:\Windows\Globalization\Sorting\SortDefault.nls Opens: C:\Users\Admin\AppData\Local\Temp\PPEMAIL\ Opens:

Opens: C:\Windows\SysWOW64\mswsock.dll Opens: C:\Windows\SysWOW64\WSHTCPIP.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 HKLM\system\currentcontrolset\control\safeboot\option Opens key: Opens key: $HKLM \ system \ current control set \ control \ srp \ dll$

```
Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
                                    HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
                                     HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:
  Opens key:
                                     HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:
                                     HKLM\system\currentcontrolset\control\nls\language
  Opens key:
                                     HKLM\system\currentcontrolset\control\mui\uilanguages
                                     HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:
  Opens key:
                                     HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:
                                     HKLM\software\wow6432node\policies\microsoft\mui\settings
                                     HKLM\software\policies\microsoft\mui\settings
  Opens key:
  Opens key:
                                     HKCU\
  Opens key:
                                     HKCU\control panel\desktop\muicached\machinelanguageconfiguration
                                     HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:
  Opens key:
                                     HKCU\software\policies\microsoft\control panel\desktop
  Opens key:
                                     HKCU\control panel\desktop\languageconfiguration
  Opens kev:
                                     HKCU\control panel\desktop
  Opens key:
                                     HKCU\control panel\desktop\muicached
  Opens key:
                                     HKLM \setminus software \setminus wow 6432 node \setminus microsoft \setminus windows \setminus current version \setminus side by side
  Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:
                                     HKLM\system\currentcontrolset\control\nls\sorting\versions
                                     HKI M\
  Opens kev:
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows
nt\currentversion\diagnostics
                                    HKLM\software\wow6432node\microsoft\windows
  Opens key:
nt\currentversion\gre_initialize
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:
                                    HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
                                    HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:
  Opens key:
                                    HKLM\software\wow6432node\microsoft\ole
  Opens key:
                                     HKLM\software\wow6432node\microsoft\ole\tracing
                                    HKLM\software\microsoft\ole\tracing
  Opens key:
  Opens key:
                                    HKCU\software\classes\
  Opens key:
                                    HKCU\software\classes\wow6432node\clsid
                                    HKCR\wow6432node\clsid
  Opens key:
  Opens key:
                                     HKLM\software\wow6432node\microsoft\oleaut
  Opens key:
                                     HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:
                                    HKLM\system\currentcontrolset\control\nls\locale
  Opens key:
                                     HKLM \ system \ current controls et \ control \ nls \ locale \ alternate \ sorts
  Opens key:
                                     HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:
                                    HKLM\system\currentcontrolset\control\cmf\config
  Opens key:
                                     HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:
                                     HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
  Opens key:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
  Opens kev:
                                    HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
                                    HKLM\software\microsoft\windows
  Opens kev:
nt\currentversion\languagepack\surrogatefallback\segoe ui
  Opens key:
                                    HKLM\software\wow6432node
                                     HKLM\software\wow6432node\proland\protector plus 2000
  Opens key:
  Opens key:
                                    HKLM\software\policies\microsoft\samclient\windows
  Opens key:
                                    HKLM\software\microsoft\sqmclient\windows
  Opens key:
                                     HKLM\system\currentcontrolset\services\winsock2\parameters
                                    {\it HKLM} \ `system \ `current control set \ `services \ `winsock2 \ `parameters \ `appid\_catalog \ 'system' 
  Opens key:
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\02210642
  Opens key:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol\_catalog 9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ parameters \ protocol_catalog_entries \ protocol_catalog \ parameters \ parameters$

Opens kev:

Opens key:

Opens key:

```
Opens key:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog9 \ catalog\_entries \ 000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 00000000000001) \ (catalog\_entries \ name space\_catalog 5 \ (catalog\_entries \ 
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:
                                   HKLM\system\currentcontrolset\services\winsock\parameters
                                   HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
  Opens kev:
  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\proland\protector plus 2000\options\email scan
options
  Opens key:
                                   HKLM\software\wow6432node\proland\protector plus 2000\options\real-time
scan options\report
                                   HKLM\software\microsoft\windows nt\currentversion\image file execution
  Queries value:
options[disableusermodecallbackfilter]
  Queries value:
                                   HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  Queries value:
                                   HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
                                   HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Oueries value:
  Oueries value:
HKLM \verb|\software| policies \verb|\microsoft| windows \verb|\safer| code identifiers[transparentenabled]|
                                   HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
  Oueries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Oueries value:
                                   HKLM\svstem\currentcontrolset\control\mui\uilanguages\en-us[type]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
                                   HKCU\control panel\desktop[preferreduilanguages]
  Queries value:
                                   HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Oueries value:
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebvside[preferexternalmanifest]
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                                   HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Oueries value:
  Oueries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                                   HKLM\software\wow6432node\microsoft\windows
  Queries value:
nt\currentversion\compatibilitv32[2a66d04f3cc49ec97d27a2555c853abal
  Queries value:
                                   HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit dlls]
  Oueries value:
                                   HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Oueries value:
                                   HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
                                   HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Oueries value:
                                   HKLM\system\currentcontrolset\control\nls\locale[00000409]
                                   HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:
  Queries value:
                                   HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:
                                   HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
                                   HKLM\software\microsoft\windows
  Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:
                                   HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
```

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane5]

nt\currentversion\languagepack\surrogatefallback[plane6]

Oueries value:

Queries value:

Queries value:

```
nt\currentversion\languagepack\surrogatefallback[plane7]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane8]
 Queries value:
                       HKLM\software\microsoft\windows
\verb|nt\currentversion\languagepack\surrogatefallback[plane9]|
 Queries value:
                       HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
                      HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane11]
                       HKLM\software\microsoft\windows
 Oueries value:
nt\currentversion\languagepack\surrogatefallback[plane12]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane13]
 Oueries value:
                      HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane15]
                       HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\languagepack\surrogatefallback[plane16]
                      HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
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\00000000001[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol catalog9\catalog entries\000000000000[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:
Queries value:
Queries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog 9 \ catalog\_entries \ 0000000000006 \ [packed catalog item]
 Oueries value:
Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000008[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[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\00000000001[displaystring]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[providerid]
 Queries value:
Queries value:
HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space\_catalog 5 \ (catalog\_entries \ 000000000001[supported name space]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Queries value:
Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \cap ameters \setminus namespace\_catalog 5 \setminus catalog\_entries \setminus 000000000001[storesserviceclass info]
 Queries 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\00000000002[librarypath]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000002[supported name space]$

Oueries value:

Queries value:

Queries 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]
 Oueries value:
- 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] Oueries 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\000000000003[addressfamily]
 Oueries value:
- 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\00000000003[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo] Oueries 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\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000004 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
- 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace] Oueries 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\000000000005[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[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\000000000006[displaystring]
- Queries value: HKLMM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid] Queries value:
- WKLMNsystem\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[supportednamespace]
- 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] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
- Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]

Queries value:

HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]

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

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

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

Queries value:

 $\label{thm:local_transform} \begin{tabular}{ll} HKLM \end{tabular} $$ HKLM \end{tabular} a meters \end{tabular} $$ in sock [maxsock addrlength] $$ in sock [$

Queries value:

Queries value:

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