Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 137, Task ID: 548

Task ID: 548 Risk Level:

Date Processed: 2016-04-28 13:01:58 (UTC)

Processing Time: 61.11 seconds Virtual Environment: IntelliVM

Execution Arguments: "c:\windows\temp\9b4d5407eec5e669a16910215b954cb8.exe"

Sample ID: Type: basic admin Owner:

9b4d5407eec5e669a16910215b954cb8 Label:

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

File Size: 340776 bytes

9b4d5407eec5e669a16910215b954cb8 MD5:

eb6dcb3f3f2189b1fe35b7822050729fc22a00ec3b48c39173895d6a8144a4fd SHA256:

Description: None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\9b4d5407eec5e669a16910215b954cb8.exe

["C:\windows\temp\9b4d5407eec5e669a16910215b954cb8.exe"]

Named Object Events

\Sessions\1\BaseNamedObjects\DBWinMutex Creates mutex:

Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0

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

File System Events

C:\Windows\Prefetch\9B4D5407EEC5E669A16910215B954-623A1966.pf Opens:

Opens: C:\Windows\System32

Opens: C:\windows\temp\WSOCK32.dll Opens: C:\Windows\System32\wsock32.dll

Opens: C:\windows\temp\9b4d5407eec5e669a16910215b954cb8.exe.Local\

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

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

C:\Windows\winsxs\x86_microsoft.windows.commoncontrols_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

C:\Windows\System32\sechost.dll Opens: Opens: C:\windows\temp\WINSPOOL.DRV Opens: C:\Windows\System32\winspool.drv C:\Windows\System32\imm32.dll Opens: Opens: C:\Windows\System32\uxtheme.dll Opens: C:\windows\temp\dwmapi.dll C:\Windows\System32\dwmapi.dll Opens: Opens: C:\Windows\Fonts\StaticCache.dat Opens: C:\Windows\System32\en-US\user32.dll.mui C:\Windows\Globalization\Sorting\SortDefault.nls Opens:

Opens: C:\windows\temp\urlswmr.txt

Opens: C:\

C:\Windows\Fonts\sserife.fon Opens: Opens: C:\windows\temp\RICHED32.DLL Opens: C:\Windows\System32\riched32.dll Opens: C:\windows\temp\RICHED20.dll Opens: C:\Windows\System32\riched20.dll C:\Windows\win.ini Opens:

Opens: C:\Windows\System32\rpcss.dll Opens: C:\windows\temp\CRYPTBASE.dll Opens: C:\Windows\System32\cryptbase.dll Opens: C:\Windows\System32\mswsock.dll Opens: C:\Windows\System32\WSHTCPIP.DLL Reads from: C:\Windows\Fonts\StaticCache.dat

C:\Windows\win.ini Reads from:

Windows Registry Events

Creates key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms

Creates key: HKCU\software\microsoft\netshow\player\general

HKCU\software Creates kev:

Creates key: HKCU\software\microsoft Creates key: HKCU\software\microsoft\netshow HKCU\software\microsoft\netshow\player Creates key: Creates key: HKCU\software\microsoft\netshow\player\local

```
HKLM\system\currentcontrolset\control\session manager
 Opens key:
 Opens key:
                     HKLM\system\currentcontrolset\control\terminal server
 Opens kev:
                     HKLM\system\currentcontrolset\control\safeboot\option
 Opens key:
                     HKLM\system\currentcontrolset\control\srp\gp\dll
 Opens key:
                     HKLM\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                     HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:
                     HKCU\control panel\desktop\muicached\machinelanguageconfiguration
 Opens key:
 Opens key:
                     HKLM\software\policies\microsoft\mui\settings
                     HKCU\software\policies\microsoft\control panel\desktop
 Opens key:
                     HKCU\control panel\desktop\languageconfiguration
 Opens key:
 Opens key:
                     HKCU\control panel\desktop
 Opens key:
                     HKCU\control panel\desktop\muicached
 Opens key:
                     HKLM\software\microsoft\windows\currentversion\sidebyside
 Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key:
                     HKI M\system\currentcontrolset\control\nls\sorting\versions
 Opens key:
                     HKLM\system\currentcontrolset\control\error message instrument\
 Opens key:
                     HKLM\system\currentcontrolset\control\error message instrument
 Opens key:
                     \label{lem:hklm} \verb+Kklm\+ software\+ microsoft\+ windows nt\+ current version\+ gre\_initialize
 Opens key:
                     HKLM\software\microsoft\windows nt\currentversion\compatibility32
 Opens key:
                     HKLM\software\microsoft\windows nt\currentversion\ime compatibility
                     HKI M\
 Opens kev:
 Opens key:
                     HKLM\software\microsoft\windows nt\currentversion\windows
 Opens key:
                     HKLM\software\microsoft\windows nt\currentversion\diagnostics
 Opens key:
                     HKLM\software\microsoft\ole
 Opens key:
                     HKLM\software\microsoft\ole\tracing
 Opens key:
                     HKLM\software\microsoft\oleaut
                     HKLM\system\currentcontrolset\services\crypt32
 Opens key:
 Opens key:
                     HKLM\software\microsoft\windows\currentversion\internet settings
 Opens key:
                     HKLM\software\policies\microsoft\windows\currentversion\internet
settings
 Opens key:
                     HKLM\system\currentcontrolset\control\nls\customlocale
 Opens key:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale
                     HKLM\system\currentcontrolset\control\nls\locale
 Opens key:
 Opens key:
                     HKLM \ system \ current controls et \ control \ nls \ locale \ alternate \ sorts
 Opens key:
                     HKLM\system\currentcontrolset\control\nls\language groups
                     \label{lem:hklm} \verb+KLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
 Opens key:
 Opens key:
                     HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
                     HKLM\software\microsoft\windows
 Opens key:
nt\currentversion\languagepack\surrogatefallback
                     HKLM\software\microsoft\windows
 Opens kev:
nt\currentversion\languagepack\surrogatefallback\segoe ui
 Opens key:
                     HKLM\system\currentcontrolset\control\cmf\config
 Opens key:
                     HKLM\software\policies\microsoft\sqmclient\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 kev:
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\07e9109d
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000019
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens kev:
Opens key:
Opens kev:
Opens key:
Opens kev:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
Opens kev:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011

Opens kev:

Opens key:

Opens kev:

Opens key:

Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000015 Opens kev:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 0000000000016$ Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000018 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000005

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006

Opens kev: HKCU\software\microsoft\windows nt\currentversion\windows

Opens key:

HKLM\software\microsoft\ctf\compatibility\9b4d5407eec5e669a16910215b954cb8.exe HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-Opens key: Ofb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

Opens key: HKLM\software\microsoft\ctf\

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

Opens key: Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock HKLM\system\currentcontrolset\services\psched\parameters\winsock Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock\setup migration\providers

Opens key: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\psched

Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

HKLM\system\currentcontrolset\services\winsock\setup Opens kev:

migration\providers\tcpip

Opens key: HKCU\software\microsoft\mediaplayer\preferences

Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http $\label{lem:hkcu} \mbox{HKCU\software\mbox{\sc hicrosoft\mbox{\sc hediaplayer\preferences\proxysettings\mbox{\sc hmms}}} \\$ Opens key: Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp

HKCU\software\microsoft\netshow\player\general Opens kev: Opens key: HKCU\software\microsoft\netshow\player\local 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] Queries value:

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Oueries value: HKCU\control panel\desktop[preferreduilanguages]

Oueries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value:

 $HKLM \verb|\software\microsoft\windows \verb|\currentversion\side| preferex ternal manifest| \\$ Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]

HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] Oueries value:

HKLM\software\microsoft\windows Queries value: nt\currentversion\gre_initialize[disablemetafiles] HKLM\software\microsoft\windows Oueries value:

nt\currentversion\compatibility32[9b4d5407eec5e669a16910215b954cb8]

Queries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value: Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags] HKLM\software\microsoft\windows\currentversion\internet Oueries value:

settings[disableimprovedzonecheck]

Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet

settings[security_hklm_only]

HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] HKLM\system\currentcontrolset\control\nls\locale[00000409] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Oueries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\datastore_v1.0[disable] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\datastore_v1.0[datafilepath]

Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2] HKLM\software\microsoft\windows Oueries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane3]|$ HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane4] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane5] HKLM\software\microsoft\windows Oueries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane6]|$ HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane7] HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane8] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane9] HKLM\software\microsoft\windows Queries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane10]|$ HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane11] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane12] HKLM\software\microsoft\windows Queries value: $\verb|nt\currentversion\languagepack\surrogatefallback[plane13]|$ HKLM\software\microsoft\windows Queries value: nt\currentversion\languagepack\surrogatefallback[plane14] Oueries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane15] HKLM\software\microsoft\windows Oueries value: nt\currentversion\languagepack\surrogatefallback[plane16] HKLM\system\currentcontrolset\control\cmf\config[system] Queries value: Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable] 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] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]

Queries value:

Queries value.

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog 9 \ catalog_entries \ 00000000000002 \ [packed catalog item] \ Queries \ value:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem] Queries 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\000000000008[packedcatalogitem] Oueries 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\000000000011[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[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\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\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 \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath] Oueries value:
- 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]
 Queries 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\0000000000002[supportednamespace]
 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]
- 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\00000000003[version]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo] Queries 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]
- 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\000000000004[supportednamespace]
- 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]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Queries 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\00000000005[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:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus amespace_catalog 5 \setminus catalog_entries \setminus 0000000000005 [enabled]$

Queries 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\00000000005[storesserviceclassinfo] Oueries value:

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:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerid]
Queries 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]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]

Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]

Queries value: HKCU\software\microsoft\windows

 $\verb|nt\currentversion\windows[scrollinterval]|$

Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-

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

Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]

 $Queries\ value: \\ HKLM\system\currentcontrolset\services\winsock\parameters[transports]$

Queries value:

Queries value:

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

migration\providers\psched[winsock 2.0 provider id]

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:

 $HKLM \setminus system \setminus current controls et \setminus services \setminus tcpip \setminus parameters \setminus winsock [maxsock addrlength]$

Queries value:

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

Queries value:

Sets/Creates value:

 $\label{local-const-mediaplayer-local-const-mediaplay$

Sets/Creates value:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyport]
Sets/Creates value:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxystyle]
Sets/Creates value:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxybypass]
Sets/Creates value:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyname]
Sets/Creates value:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyhost]
 Sets/Creates value:

 $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus preferences \setminus proxysettings \setminus rtsp[proxyhost]$

HKCU\software\microsoft\netshow\player\general[enablehttp] Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enabletcp] Sets/Creates value: Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enableudp] HKCU\software\microsoft\netshow\player\general[enablemulticast] Sets/Creates value: HKCU\software\microsoft\netshow\player\general[firstprotocol] Sets/Creates value: Sets/Creates value: HKCU\software\microsoft\netshow\player\local[appliedautoproxy] HKCU\software\microsoft\netshow\player\local[enableautoproxy] Sets/Creates value: Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyenabled]

Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyname]
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyhost]
Sets/Creates value: HKCU\software\microsoft\netshow\player\local[proxyport]
Value changes:

 $\label{thm:local_HKCU} HKCU \software \microsoft \mediaplayer \preferences \proxy settings \http[proxy port] \\ Value \ changes:$

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxystyle]
 Value changes:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxybypass]
 Value changes:

 $\label{thm:local_HKCU} HKCU \software \microsoft \mediaplayer \preferences \proxysettings \http[proxyname] \\ Value \ changes:$

 $\label{lem:hkcu} HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxyport] \\ Value\ changes:$

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxystyle]
 Value changes:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxybypass]
 Value changes:

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxyname]