Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 137, Task ID: 547

Task ID: 547 Risk Level: 1

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

Processing Time: 61.2 seconds
Virtual Environment: IntelliVM

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

Sample ID: 137
Type: basic
Owner: admin

Label: 9b4d5407eec5e669a16910215b954cb8

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

File Type: PE32:win32:gui File Size: 340776 bytes

MD5: 9b4d5407eec5e669a16910215b954cb8

SHA256: eb6dcb3f3f2189b1fe35b7822050729fc22a00ec3b48c39173895d6a8144a4fd

Description: None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\9b4d5407eec5e669a16910215b954cb8.exe

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

Named Object Events

Creates mutex: \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003 Creates mutex:

\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003 Creates mutex:

\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-

1957994488-1003

Creates mutex: \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003

Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens: C:\WINDOWS\Prefetch\9B4D5407EEC5E669A16910215B954-0733C257.pf

Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\wsock32.dll
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\system32\comctl32.dll

Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\COMCTL32.dll.124.Config

Opens: C:\WINDOWS\system32\shell32.dll

Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83

Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-

Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comct132.dll

Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config

 Opens:
 C:\WINDOWS\system32\urlmon.dll.123.Manifest

 Opens:
 C:\WINDOWS\system32\urlmon.dll.123.Config

 Opens:
 C:\WINDOWS\system32\WININET.dll.123.Manifest

 Opens:
 C:\WINDOWS\system32\WININET.dll.123.Config

Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\windows\temp\urlswmr.txt

Opens: C:\

Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\WINDOWS\system32\riched32.dll
Opens: C:\WINDOWS\system32\riched20.dll

Opens: C:\WINDOWS\win.ini

Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll

Reads from: C:\WINDOWS\win.ini

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings

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

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

options\9b4d5407eec5e669a16910215b954cb8.exe

Opens key: HKLM\system\currentcontrol\set\control\terminal server Opens key: HKLM\system\currentcontrol\safeboot\option

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

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: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics

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

options\msvcrt.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

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\gdi32.dll

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

options\user32.dll

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

options\kernel32.dll

 $Opens~key: \\ HKLM\software\microsoft\windows~nt\currentversion\cite{Linear} index~equivolution for the continuous conti$

options\comctl32.dll

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

options\shlwapi.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\shell32.dll

Opens key:

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\comdlg32.dll
 Opens key:

 $\label{lem:hklmsoftware} \begin{tabular}{ll} HKLM\software\mbox{\mbox{microsoft$}\windows nt\currentversion\image file execution} \end{tabular}$

options\winspool.drv
 Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\normaliz.dll
 Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\ole32.dll Opens key:

Opens key:

Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\oleaut32.dll

•

options\iertutil.dll

HKLM\software\microsoft\windows nt\currentversion\image file execution
HKLM\software\microsoft\windows nt\currentversion\image file execution

options\urlmon.dll
 Opens key:

HKLM\software\microsoft\windows nt\currentversion\image file execution

options\wininet.dll

Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

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

Opens key: HKCU\

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

Opens key: HKCU\control panel\desktop

Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance

Opens key: HKLM\system\setup

Opens key:

 $\label{thm:linear} \begin{tabular}{ll} HKLM \end{tabular} is software \verb|\microsoft| windows \end{tabular} current version \end{tabular} is idebyside \end{tabular} as sembly storage roots \end{tabular}$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack

Opens key: HKLM\software\microsoft\ole

Opens key: HKCR\interface

Opens key: HKCR\interface\{00020400-0000-c000-000000000046}

Opens key: HKLM\software\microsoft\oleaut

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

HKCU\software\classes\ Opens key: Opens key: HKCU\software\classes\protocols\name-space handler\ Opens key: HKCR\protocols\name-space handler HKCU\software\classes\protocols\name-space handler Opens key: Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings Opens key: HKLM\software\microsoft\windows\currentversion\internet settings HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\ Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol Opens kev: HKCU\software\policies\microsoft\internet explorer\main\featurecontrol Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol Opens key: HKCU\software\microsoft\internet explorer\main\featurecontrol HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings\zonemap\domains\ $\label{lem:hkcu} \verb+KKCU\+ software\+ policies\+ microsoft\+ windows\+ current version\+ internet$ Opens key: settings\zonemap\domains\ HKLM\software\policies\microsoft\windows\currentversion\internet Opens key: settings\zonemap\ranges\ Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet settings\zonemap\ranges\ HKCU\software\microsoft\internet Opens key: explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_unc_savedfilecheck Opens key: HKLM\system\currentcontrolset\control\wmi\security HKLM\software\microsoft\windows nt\currentversion\image file execution Opens kev: options\msctf.dll Opens key: HKLM\software\microsoft\ctf\compatibility\9b4d5407eec5e669a16910215b954cb8.exe Opens key: HKLM\software\microsoft\ctf\systemshared\ HKCU\keyboard layout\toggle Opens key: HKLM\software\microsoft\ctf\ Opens kev: HKLM\software\microsoft\windows nt\currentversion\imm Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\version.dll $\label{thm:local_hammon_hammon} \begin{tabular}{l} HKCU \software \mbox{\mathbb{N} indows nt \current version \approx{\mathbb{N} approx \mathbb{N} approx \mathbb{N} approx{\mathbb{N} approx \mathbb{N} appro$ Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime Opens key: HKCU\software\microsoft\ctf Opens key: ${\it HKLM \backslash software \backslash microsoft \backslash ctf \backslash systems hared}$ $HKLM \verb|\system| current control set \verb|\services| winsock 2 \verb|\parameters| \\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9 Opens kev: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004 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 key: Opens key: Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000007 Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000000 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010 Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000011 Opens key:

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004 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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\riched20.dll Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\riched32.dll HKCU\software\microsoft\windows nt\currentversion\windows Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\mswsock.dll HKLM\software\microsoft\windows nt\currentversion\image file execution Opens key: options\hnetcfg.dll Opens key: HKLM\software\microsoft\rpc\pagedbuffers HKLM\software\microsoft\rpc Opens key: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\9b4d5407eec5e669a16910215b954cb8.exe\rpcthreadpoolthrottle Opens kev: HKLM\software\policies\microsoft\windows nt\rpc 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 kev: HKCU\software\microsoft\mediaplayer\preferences Opens key: Opens key: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms $\label{lem:hkcu} \mbox{HKCU\software\mbox{$\mbox{microsoft\mbox{$\mbox{}\mbox{$\mbox{\mbox Opens key: Opens key: HKCU\software\microsoft\netshow\player\general Opens key: HKCU\software\microsoft\netshow\player\local HKLM\system\currentcontrolset\control\terminal server[tsappcompat] Oueries value: Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled] HKLM\system\currentcontrolset\control\terminal server[tsuserenabled] Oueries value: Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack] Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode] HKLM\software\microsoft\windows Oueries value: nt\currentversion\gre_initialize[disablemetafiles] Oueries value: HKLM\software\microsoft\windows $\verb|nt\currentversion\compatibility| 32[9b4d5407eec5e669a16910215b954cb8]|$ HKLM\software\microsoft\windows nt\currentversion\ime Oueries value: compatibility[9b4d5407eec5e669a16910215b954cb8] $\label{thm:local_hammon_hammon} \begin{tabular}{ll} HKLM\software\mbox{\sc microsoft\windows nt\currentversion\windows[appinit_dlls]} \end{tabular}$ Oueries value: Queries value: HKCU\control panel\desktop[multiuilanguageid] Oueries value: HKCU\control panel\desktop[smoothscroll] Queries value: HKLM\system\setup[systemsetupinprogress] Oueries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips] Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout] HKLM\software\microsoft\ole[rwlockresourcetimeout] Oueries value: Queries value: HKCR\interface[interfacehelperdisableall] HKCR\interface[interfacehelperdisableallforole32] Queries value: HKCR\interface[interfacehelperdisabletypelib] Queries value: HKCR\interface\{00020400-0000-0000-c000-Oueries value: 00000000046}[interfacehelperdisableall] Queries value: HKCR\interface\{00020400-0000-0000-c000-00000000046}[interfacehelperdisableallforole32] $HKLM \verb|\software\microsoft\windows\currentversion\currenter|$ Queries value: settings[disableimprovedzonecheck] HKLM\software\microsoft\internet Queries value: explorer\main\featurecontrol\feature_protocol_lockdown[9b4d5407eec5e669a16910215b954cb8.exe] Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*] Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45ab78-1084642581fb] Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000000 Oueries value: HKLM\software\microsoft\ctf\systemshared[cuas] HKCU\keyboard layout\toggle[language hotkey] Oueries value: Queries value: HKCU\keyboard layout\toggle[hotkey] Oueries value: HKCU\keyboard layout\toggle[layout hotkey] Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]

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

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog@[sorial]

Queries value: Oueries value:

Oueries value:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol_catalog9 [serial_access_num]$

HKLM\software\microsoft\windows nt\currentversion\imm[ime file]

HKCU\software\microsoft\ctf[disable thread input manager]

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\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\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\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[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\000000000001[librarypath]
- 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 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]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000000002[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog 5 \ catalog_entries \ 00000000000002 \ [version] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\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:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 00000000000003 \ [supported name space]$ Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \namespace_catalog5 \catalog5 \cat$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog5 \ catalog_entries \ 000000000003 \ [storesserviceclassinfo] \ Queries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [ws 2_32 spin count]$

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

Oueries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay] Oueries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist] Oueries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelav] HKCU\software\microsoft\windows Queries value: nt\currentversion\windows[scrollinterval] Queries value: HKLM\software\microsoft\rpc[maxrpcsize] Oueries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel] HKLM\system\currentcontrolset\services\winsock\parameters[transports] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength] Oueries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance] Oueries value: HKLM\svstem\currentcontrolset\services\tcpip\parameters\winsock[helperdllname] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[usehttp] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[usetcp] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[useudp] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences[usemulticast] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\http[proxyhost] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyhost] Sets/Creates value: HKCU\software\microsoft\mediaplayer\preferences\proxysettings\rtsp[proxyhost] Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enablehttp] Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enabletcp] Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enableudp] Sets/Creates value: HKCU\software\microsoft\netshow\player\general[enablemulticast] Sets/Creates value: Sets/Creates value: HKCU\software\microsoft\netshow\player\local[appliedautoproxy]

Sets/Creates value: HKCU\software\microsoft\netshow\player\local[enableautoproxy] 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] HKLM\software\microsoft\cryptography\rng[seed] Value changes:

Value changes:

 $\label{lem:hkcu} \begin{tabular}{ll} HKCU \software \microsoft \mediaplayer \preferences \proxysettings \http[proxyport] \end{tabular}$ Value changes:

HKCU\software\microsoft\mediaplaver\preferences\proxvsettings\http[proxvstvle] Value changes:

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

 $HKCU \setminus software \setminus microsoft \setminus mediaplayer \setminus preferences \setminus proxysettings \setminus ttp[proxyname]$

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyport] Value changes:

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

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

HKCU\software\microsoft\mediaplayer\preferences\proxysettings\mms[proxyname] Value changes:

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]