Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 161, Task ID: 643

Task ID:	643
Risk Level:	5
Date Processed:	2016-04-28 13:04:49 (UTC)
Processing Time:	61.09 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe"
Sample ID:	161
Type:	basic
Owner:	admin
Label:	6282b1723f3a4b0054d80aeb27c8fed5
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	813216 bytes
MD5:	6282b1723f3a4b0054d80aeb27c8fed5
SHA256:	63e6e2e578871b03c530a3a5d3ddd22e6a00bf9de6f167ceeb5908d5c9c56c8e
Description:	None

Pattern Matching Results

2 PE: Nonstandard section
5 Packer: UPX
5 PE: Contains compressed section
4 Checks whether debugger is present

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process: C:\WINDOWS\Temp\6282b1723f3a4b0054d80aeb27c8fed5.exe ["c:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.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}
Creates semaphore: \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Creates: C:\Documents and Settings\All Users\Application Data\ZebraNetworkSystems
Creates: C:\Documents and Settings\All Users\Application Data\ZebraNetworkSystems\NeoRouter
Creates: C:\Documents and Settings\Admin\Application Data\ZebraNetworkSystems
Creates: C:\Documents and Settings\Admin\Application Data\ZebraNetworkSystems\NeoRouter
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\{AB5C856A-A12F-44A9-AE06-4A1DA4BEC313}
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\Tmp1.tmp
Opens: C:\WINDOWS\Prefetch\6282B1723F3A4B0054D80AEB27C8F-2D7629E3.pf
Opens: C:\Documents and Settings\Admin
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\comctl32.dll
Opens: C:\WINDOWS\system32\crypt32.dll
Opens: C:\WINDOWS\system32\msasn1.dll
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\wsock32.dll
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.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\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\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.2.Manifest
Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.3.Manifest
Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.Manifest
Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.Config
Opens: C:\windows\temp\Log.ini
Opens: C:\Documents and Settings\All Users\Application Data\ZebraNetworkSystems\NeoRouter\Log.ini
Opens: C:\windows\temp\6282b1723f3a4b0054d80aeb27c8fed5.exe.1000.Manifest
Opens: C:\dev\
Opens: C:\WINDOWS\system32\netapi32.dll
Opens: C:\WINDOWS\system32\rsaenh.dll
Opens: C:\usr\local\ssl\cert.pem
Opens: C:\WINDOWS\system32\mswsock.dll
Opens: C:\WINDOWS\system32\dnsapi.dll
Opens: C:\WINDOWS\system32\iphlpapi.dll
Opens: C:\WINDOWS\system32\drivers\etc\hosts
Opens: C:\WINDOWS\system32\hnetcfg.dll
Opens: C:\WINDOWS\system32\wshtcpip.dll
Opens: C:\WINDOWS\system32\rasadhlp.dll
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\uxtheme.dll
Reads from: C:\WINDOWS\system32\rsaenh.dll
Reads from: C:\WINDOWS\system32\drivers\etc\hosts

Network Events

DNS query: secure.neorouter.com
Sends data to: 8.8.8.8:53

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\internet settings
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders
Creates key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\6282b1723f3a4b0054d80aeb27c8fed5.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
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\user32.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\gdi32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shlwapi.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comctl32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\msasn1.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
Opens key: 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\software\microsoft\windows nt\currentversion\image file execution
options\winspool.drv
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\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: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\system\setup
Opens key: HKLM\system\currentcontrolset\services\crypt32\performance
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\oleaut\userera
Opens key: HKCU\software\classes\
Opens key: HKCU\software\classes\protocols\name-space handler\
Opens key: HKCR\protocols\name-space handler
Opens key: HKCU\software\classes\protocols\name-space handler
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
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
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
Opens key: HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
Opens key: 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
Opens key: HKCU\software\microsoft\internet
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\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
Opens key: HKCU\software\microsoft\internet
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
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
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\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\network
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
Opens key: HKLM\software\microsoft\rpc\pagedbuffers
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6282b1723f3a4b0054d80aeb27c8fed5.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKCU\software\microsoft\cryptography\providers\type 001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider types\type 001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\intel hardware
cryptographic service provider
Opens key: HKLM\software\zebranetworksystems\neorouter
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
Opens key: HKLM\system\currentcontrolset\services\dnscache\parameters
Opens key: HKLM\software\policies\microsoft\windows nt\dnsclient
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
Opens key: HKLM\system\currentcontrolset\services\tcpip\linkage
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
Opens key: HKLM\system\currentcontrolset\services\netbt\parameters
Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
Opens key: HKLM\software\policies\microsoft\system\dnsclient
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
Opens key: HKLM\software\microsoft\rpc\securityservice
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\wshtcpip.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\rasadhlp.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\6282b1723f3a4b0054d80aeb27c8fed5.exe
Opens key: HKLM\software\microsoft\ctf\systemshared\
Opens key: HKCU\keyboard layout\toggle
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\imm
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\version.dll
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctfime.ime
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[6282b1723f3a4b0054d80aeb27c8fed5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[6282b1723f3a4b0054d80aeb27c8fed5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[6282b1723f3a4b0054d80aeb27c8fed5.exe]
Queries value: HKLM\software\microsoft\internet explorer\main\featurecontrol\feature_protocol_lockdown[*]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-ab78-1084642581fb]
Queries value: HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-0000-000000000000]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
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: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries 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]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries 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\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
Queries 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]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries 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\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries 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\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]
Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider types\type
001[name]

Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
Queries value: HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
Queries value:

HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
Queries value: HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[enabledhcp]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseobtainedtime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[leaseterminatestime]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[queryadaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[disableadapterdomainname]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registeradaptername]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[registrationmaxaddresscount]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[maxnumberofaddressestoregister]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[domain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpdomain]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[ipautoconfigurationenabled]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[addresstype]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[nameserver]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-c7d49d7cecdc}[dhcpnameserver]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
Queries value: HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
Queries value: HKLM\system\currentcontrolset\services\winsock\parameters[transports]
Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]

Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]