Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3312, Task ID: 755

Task ID:	755
Risk Level:	10
Date Processed:	2016-05-18 10:34:11 (UTC)
Processing Time:	62.79 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"
Sample ID:	3312
Type:	basic
Owner:	admin
Label:	859ba9477553ccad1bba34c555ab6a1b
Date Added:	2016-05-18 10:30:49 (UTC)
File Type:	PE32:win32:gui
File Size:	199680 bytes
MD5:	859ba9477553ccad1bba34c555ab6a1b
SHA256:	339ff6766efd4c5f26a8c0c9413b68ae664bb5eb8dfa403bec5df2909cbb73a1
Description:	None

Pattern Matching Results

7 Writes to memory of system processes
6 Modifies registry autorun entries
6 Writes to system32 folder
2 PE: Nonstandard section
5 Abnormal sleep detected
7 Injects thread into Windows process
3 HTTP connection - response code 200 (success)
6 Changes Winsock providers
10 Creates malicious events: ZeroAccess [Rootkit]
4 Terminates process under Windows subfolder
4 Reads process memory
5 PE: Contains compressed section
3 Long sleep detected
5 Installs service

Static Events

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process: C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe ["C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"]
Creates process: C:\Windows\SysWOW64\cmd.exe ["C:\Windows\system32\cmd.exe"]
Creates process: \SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
Reads from process: PID:1680 C:\Windows\SysWOW64\calc.exe
Writes to process: PID:2044 C:\Windows\explorer.exe
Writes to process: PID:480 C:\Windows\System32\services.exe
Writes to process: PID:1300 C:\Windows\SysWOW64\cmd.exe
Terminates process: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
Terminates process: C:\Windows\System32\rundll32.exe
Terminates process: C:\Windows\SysWOW64\cmd.exe
Terminates process: C:\Windows\System32\conhost.exe
Creates remote thread: C:\Windows\explorer.exe
Creates remote thread: C:\Windows\System32\services.exe

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates event: \Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event: \Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event: \BaseNamedObjects\\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}

File System Events

Creates: C:\$Recycle.Bin\
Creates: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001
Creates: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3
Creates: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\L
Creates: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\U
Creates: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\@

Creates: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
Creates: C:\$Recycle.Bin\S-1-5-18
Creates: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3
Creates: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\L
Creates: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\U
Creates: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
Creates: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
Creates: C:GAC_MSIL
Creates: C:\Windows\assembly\GAC
Creates: C:GAC_32
Creates: C:GAC_64
Creates: C:\Windows\assembly\GAC_64\Desktop.ini
Creates: C:\Windows\assembly\GAC_32\Desktop.ini
Creates: C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
Creates: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles
Opens: C:\Windows\Prefetch\859BA9477553CCAD1BBA34C555AB6-401FB0A4.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
Opens: C:\Windows\SysWOW64\ntdll.dll
Opens: C:\Windows\SysWOW64\kernel32.dll
Opens: C:\Windows\SysWOW64\KernelBase.dll
Opens: C:\Windows\apppatch\sysmain.sdb
Opens: C:\Windows\SysWOW64\atl.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\msvcrt.dll
Opens: C:\Windows\SysWOW64\shlwapi.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\Windows\SysWOW64\bcryptprimitives.dll
Opens: C:\Windows\SysWOW64\cryptbase.dll
Opens: C:\Windows\SysWOW64\sspicli.dll
Opens: C:\Windows\SysWOW64\rpcrt4.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\cabinet.dll
Opens: C:\Windows\SysWOW64\nsi.dll
Opens: C:\Windows\SysWOW64\ws2_32.dll
Opens: C:\Windows\SysWOW64\mswsock.dll
Opens: C:\Windows\SysWOW64\cryptsp.dll
Opens: C:\Windows\SysWOW64\rsaenh.dll
Opens: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
Opens: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
Opens: C:\Windows\assembly
Opens: C:\Windows\assembly\GAC_32\Desktop.ini
Opens: C:\Windows\assembly\GAC_64\Desktop.ini
Opens: C:\Windows\System32\cryptsp.dll
Opens: C:\Windows\System32\rsaenh.dll
Opens: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
Opens: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\U
Opens: C:\Windows\SysWOW64\cmd.exe
Opens: C:\
Opens: C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Opens: C:
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting
Opens: C:\Windows\System32
Opens: C:\Windows\SysWOW64\wbem
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\locale.nls
Opens: C:\Windows\SysWOW64\wbem\WMIC.exe
Opens: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\@
Opens: C:\Windows\System32\conhost.exe
Opens: C:\Windows\System32\combase.dll
Opens: C:\Windows\System32\en-US\conhost.exe.mui
Opens: C:\Windows\System32\ole32.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\Windows\System32\cmd.exe
Opens: C:\Windows\System32\en-US\cmd.exe.mui
Opens: C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
Opens: C:\Windows\System32\LogFiles\Scm\e4dfe66f-e089-4cc3-a70f-957223d565f4
Opens:

C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
Writes to: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\@
Writes to: C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
Writes to: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
Writes to: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
Writes to: C:\Windows\assembly\GAC_64\Desktop.ini
Writes to: C:\Windows\assembly\GAC_32\Desktop.ini
Writes to: C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
Reads from: C:\Windows\SysWOW64\cmd.exe
Reads from: C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Reads from: C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
Reads from: C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
Reads from: C:\Windows\System32\LogFiles\Scm\e4dfe66f-e089-4cc3-a70f-957223d565f4
Reads from: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
Deletes: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Network Events

DNS query: promos.fling.com
DNS response: promos.fling.com ⇒ 208.91.207.58
Connects to: 208.91.207.58:80
Connects to: 213.108.252.185:80
Sends data to: 8.8.8.8:53
Sends data to: promos.fling.com:80 (208.91.207.58)
Sends data to: 83.133.123.20:53
Sends data to: 213.108.252.185:80
Sends data to: 66.169.64.252:16470
Sends data to: 70.245.30.44:16470
Sends data to: 24.166.74.57:16470
Sends data to: 84.238.123.251:16470
Sends data to: 98.200.159.59:16470
Sends data to: 24.166.102.61:16470
Sends data to: 207.253.171.66:16470
Sends data to: 76.90.0.73:16470
Sends data to: 99.250.124.73:16470
Sends data to: 90.129.15.104:16470
Sends data to: 207.98.234.114:16470
Sends data to: 75.177.68.122:16470
Sends data to: 209.20.29.125:16470
Sends data to: 98.203.59.126:16470
Sends data to: 98.223.143.132:16470
Sends data to: 68.44.66.138:16470
Sends data to: 67.183.232.147:16470
Sends data to: 81.233.194.148:16470
Sends data to: 90.237.150.151:16470
Sends data to: 76.17.49.27:16470
Sends data to: 75.71.170.178:16470
Sends data to: 94.191.193.25:16470
Sends data to: 64.244.39.17:16470
Sends data to: 190.172.245.16:16470
Sends data to: 70.66.158.194:16470
Sends data to: 180.215.28.200:16470
Sends data to: 62.143.199.5:16470
Sends data to: 68.35.93.217:16470
Sends data to: 24.7.243.232:16470
Sends data to: 76.84.200.232:16470
Sends data to: 113.211.25.228:16470
Sends data to: 108.162.165.226:16470
Sends data to: 65.26.156.226:16470
Sends data to: 184.58.36.223:16470
Sends data to: 202.147.221.2:16470
Sends data to: 83.254.124.221:16470
Sends data to: 121.73.119.3:16470
Sends data to: 206.174.8.235:16470
Sends data to: 173.179.2.4:16470
Sends data to: 81.233.3.4:16470
Sends data to: 176.198.31.4:16470
Sends data to: 89.239.230.213:16470
Sends data to: 24.252.143.4:16470
Sends data to: 189.106.146.212:16470
Sends data to: 24.223.187.210:16470
Sends data to: 24.60.167.210:16470
Sends data to: 70.80.21.5:16470
Sends data to: 96.22.40.5:16470
Sends data to: 68.224.54.5:16470
Sends data to: 113.35.220.208:16470
Sends data to: 107.9.219.208:16470
Sends data to: 68.59.113.5:16470
Sends data to: 87.50.25.235:16470
Sends data to: 62.75.219.6:16470

Receives data from: 0.0.0.0:0
Receives data from: promos.fling.com:80 (208.91.207.58)
Receives data from: 213.108.252.185:80

Windows Registry Events

Creates key: HKCU\software\classes\clsid
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
Deletes value: HKLM\software\microsoft\windows\currentversion\run[windows defender]
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\disable8and16bitmitigation
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
Opens key: HKLM\software\wow6432node\microsoft\windows 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
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\system\currentcontrolset\control\compression
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2f2e863f
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
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:
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\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000014
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:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
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\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:
HKLM\software\policies\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key:
HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-
a949-c1b91af43b1a}
Opens key: HKLM\software\microsoft\windows\currentversion\run
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\software\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows nt\currentversion
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\conhost.exe
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\system\currentcontrolset\services\bfe\startoverride
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\alg
Opens key: HKLM\system\currentcontrolset\services\alg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\alluserinstallagent
Opens key: HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\appidsvc
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\appinfo
Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt
Opens key: HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\axinstsv
Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bits\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\brokerinfrastructure
Opens key: HKLM\system\currentcontrolset\services\brokerinfrastructure\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser

Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\browser\startoverride
Opens key: HKLM\system\currentcontrolset\services\bthserv
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\certpropsvc
Opens key: HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\comsysapp
Opens key: HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\cryptsvc
Opens key: HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\cscservice
Opens key: HKLM\system\currentcontrolset\services\cscservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\cscservice\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\defragsvc
Opens key: HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\deviceassociationservice
Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo
Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0
Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1
Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\deviceinstall
Opens key: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\dhcp
Opens key: HKLM\system\currentcontrolset\services\dhcp\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
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\system\currentcontrolset\control\cmf\config
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
Opens key: HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
Opens key: HKLM\system\currentcontrolset\services\dnscache\startoverride
Opens key: HKCU\console
Opens key: HKCU\console\
Opens key: HKLM\system\currentcontrolset\services\dot3svc
Opens key: HKLM\system\currentcontrolset\services\dot3svc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dps
Opens key: HKLM\system\currentcontrolset\services\dps\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dsmsvc
Opens key: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\eaphost
Opens key: HKLM\system\currentcontrolset\services\eaphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eventsystem
Opens key: HKLM\system\currentcontrolset\services\eventsystem\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fax
Opens key: HKLM\system\currentcontrolset\services\fax\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fdphost
Opens key: HKLM\system\currentcontrolset\services\fdphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fdrespub
Opens key: HKLM\system\currentcontrolset\services\fdrespub\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fhsvc
Opens key: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\fontcache
Opens key: HKLM\system\currentcontrolset\services\fontcache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\gpsvc
Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\hidserv
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\hkmsvc
Opens key: HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ikeext
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ikeext\startoverride
Opens key: HKLM\system\currentcontrolset\services\ivmservice
Opens key: HKLM\system\currentcontrolset\services\keyiso
Opens key: HKLM\system\currentcontrolset\services\keyiso\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ktmrm
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lanmanserver
Opens key: HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lltdsvc
Opens key: HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lmhosts
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\3
Opens key: HKLM\system\currentcontrolset\services\lsm
Opens key: HKLM\system\currentcontrolset\services\lsm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\mmcss
Opens key: HKLM\system\currentcontrolset\services\mmcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msdtc
Opens key: HKLM\system\currentcontrolset\services\msdtc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msiscsi
Opens key: HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msiserver
Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\napagent
Opens key: HKLM\system\currentcontrolset\services\napagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ncasvc
Opens key: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\3
Opens key: HKLM\system\currentcontrolset\services\ncdautosetup
Opens key: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\netlogon
Opens key: HKLM\system\currentcontrolset\services\netlogon\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netman
Opens key: HKLM\system\currentcontrolset\services\netman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netprofm
Opens key: HKLM\system\currentcontrolset\services\netprofm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nlasvc
Opens key: HKLM\system\currentcontrolset\services\nlasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nsi
Opens key: HKLM\system\currentcontrolset\services\nsi\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ose
Opens key: HKLM\system\currentcontrolset\services\ose\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2psvc
Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pcasvc
Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\perfhost
Opens key: HKLM\system\currentcontrolset\services\perfhost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pla
Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\plugplay
Opens key: HKLM\system\currentcontrolset\services\plugplay\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\policyagent\startoverride
Opens key: HKLM\system\currentcontrolset\services\power
Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\printnotify
Opens key: HKLM\system\currentcontrolset\services\printnotify\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\profsvc
Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\qwave
Opens key: HKLM\system\currentcontrolset\services\qwave\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rasauto
Opens key: HKLM\system\currentcontrolset\services\rasauto\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rasman
Opens key: HKLM\system\currentcontrolset\services\rasman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteaccess
Opens key: HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteregistry
Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpclocator
Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpcss
Opens key: HKLM\system\currentcontrolset\services\rpcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\samss
Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\scardsvr
Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\schedule
Opens key: HKLM\system\currentcontrolset\services\schedule\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sdrsvc
Opens key: HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\seclogon
Opens key: HKLM\system\currentcontrolset\services\seclogon\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sens
Opens key: HKLM\system\currentcontrolset\services\sens\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\3
Opens key: HKLM\system\currentcontrolset\services\sessionenv
Opens key: HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\shellhwdetection
Opens key: HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\snmptrap
Opens key: HKLM\system\currentcontrolset\services\snmptrap\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\spooler
Opens key: HKLM\system\currentcontrolset\services\spooler\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sppsvc
Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0

Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sstpsvc
Opens key: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\stisvc
Opens key: HKLM\system\currentcontrolset\services\stisvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\svsvc
Opens key: HKLM\system\currentcontrolset\services\svsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\swprv
Opens key: HKLM\system\currentcontrolset\services\swprv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sysmain
Opens key: HKLM\system\currentcontrolset\services\sysmain\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\systemeventsbroker
Opens key: HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\tapisrv
Opens key: HKLM\system\currentcontrolset\services\tapisrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\termservice
Opens key: HKLM\system\currentcontrolset\services\termservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\themes
Opens key: HKLM\system\currentcontrolset\services\themes\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\threadorder
Opens key: HKLM\system\currentcontrolset\services\threadorder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\timebroker
Opens key: HKLM\system\currentcontrolset\services\timebroker\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\tlntsvr
Opens key: HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\trkwks
Opens key: HKLM\system\currentcontrolset\services\trkwks\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\trustedinstaller
Opens key: HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ui0detect
Opens key: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\umrdpservice
Opens key: HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\upnphost
Opens key: HKLM\system\currentcontrolset\services\upnphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vaultsvc
Opens key: HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vds
Opens key: HKLM\system\currentcontrolset\services\vds\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmicheartbeat
Opens key: HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\vmickvpexchange
Opens key: HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\vmicrdv
Opens key: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\vmicshutdown
Opens key: HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\vmictimesync
Opens key: HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\vmicvss
Opens key: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\vss
Opens key: HKLM\system\currentcontrolset\services\vss\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\w32time
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wbengine
Opens key: HKLM\system\currentcontrolset\services\wbengine\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcmsvc
Opens key: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wcncsvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wdiservicehost
Opens key: HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\webclient
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wecsvc
Opens key: HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wercplsupport
Opens key: HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wiarpc
Opens key: HKLM\system\currentcontrolset\services\wiarpc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\windefend
Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\windefend\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\winmgmt
Opens key: HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\winrm
Opens key: HKLM\system\currentcontrolset\services\winrm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wlansvc
Opens key: HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wlidsvc
Opens key: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wmiapsrv
Opens key: HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpcsvc
Opens key: HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\5
Opens key: HKLM\system\currentcontrolset\services\wsearch
Opens key: HKLM\system\currentcontrolset\services\wsearch\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wsservice
Opens key: HKLM\system\currentcontrolset\services\wsservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wsservice\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wuauserv
Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wudfsvc
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wwansvc
Opens key: HKLM\system\currentcontrolset\services\wwansvc\triggerinfo

Opens key: HKCU\console\%systemroot%_system32_cmd.exe
Opens key: HKCU\console\%systemroot%\system32\cmd.exe
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32
Opens key: HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler
Opens key: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler
Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
Opens key: HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
Opens key: HKLM\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\policies\microsoft\windows\edgeui
Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
Opens key: HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
Opens key: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
Opens key: HKCU\software\classes\applications\calc.exe
Opens key: HKCR\applications\calc.exe
Opens key: HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}
Opens key: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}
Opens key: HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\treatas
Opens key: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\treatas
Opens key: HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32
Opens key: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32
Opens key: HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler32
Opens key: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler32
Opens key: HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler
Opens key: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
Opens key: HKCU\software\classes\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
Opens key: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
Opens key: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\
Opens key: HKCU\software\classes\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellex\iconhandler
Opens key: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\shellex\iconhandler
Opens key: HKCU\software\classes\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\defaulticon
Opens key: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\defaulticon
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\namecustomizations
Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\ctf\knownclasses

Opens key: HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
Opens key: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
Opens key: HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
Opens key: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
Opens key: HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32
Opens key: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32
Opens key: HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler32
Opens key: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler32
Opens key: HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler
Opens key: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler
Opens key: HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}
Opens key: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}
Opens key: HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\treatas
Opens key: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\treatas
Opens key: HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32
Opens key: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32
Opens key: HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler32
Opens key: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler32
Opens key: HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler
Opens key: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler
Opens key: HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value: HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[859ba9477553ccad1bba34c555ab6a1b.exe]
Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[859ba9477553ccad1bba34c555ab6a1b]
Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries 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: 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\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\000000000001[providerinfo]
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\000000000002[providerinfo]
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\namespace_catalog5\catalog_entries\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
Queries 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]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:
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]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries 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]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries 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\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries 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]
Queries 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\tcpip\parameters\winsock[mapping]
Queries value: HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
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\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[image path]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\windows[displayversion]
Queries value: HKCU\control panel\desktop[paintdesktopversion]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bfe[type]
Queries value: HKLM\system\currentcontrolset\services\bfe[start]
Queries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bfe[tag]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bfe[group]
Queries value: HKLM\system\currentcontrolset\services\bfe[objectname]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]

Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
Queries value: HKLM\system\currentcontrolset\services\browser[imagepath]
Queries value: HKLM\system\currentcontrolset\services\browser[type]
Queries value: HKLM\system\currentcontrolset\services\browser[start]
Queries value: HKLM\system\currentcontrolset\services\browser[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\browser[tag]
Queries value: HKLM\system\currentcontrolset\services\browser[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\browser[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\browser[group]
Queries value: HKLM\system\currentcontrolset\services\browser[objectname]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[action]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[type]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[data0]
Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[data0]
Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype1]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]

Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\system\currentcontrolset\services\dnscache[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dnscache[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache[start]
Queries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\dnscache[tag]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependonservice]
Queries value: HKCU\console[screencolors]
Queries value: HKCU\console[popupcolors]
Queries value: HKCU\console[insertmode]
Queries value: HKCU\console[quickedit]
Queries value: HKCU\console[codepage]
Queries value: HKCU\console[screenbuffersize]
Queries value: HKCU\console[windowsize]
Queries value: HKCU\console[windowposition]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\dnscache[group]
Queries value: HKLM\system\currentcontrolset\services\dnscache[objectname]
Queries value: HKCU\console[fontsize]
Queries value: HKCU\console[fontfamily]
Queries value: HKCU\console[fontweight]
Queries value: HKCU\console[facename]
Queries value: HKCU\console[cursorsize]
Queries value: HKCU\console[historybuffersize]
Queries value: HKCU\console[numberofhistorybuffers]
Queries value: HKCU\console[historynodup]
Queries value: HKCU\console[colortable00]
Queries value: HKCU\console[colortable01]
Queries value: HKCU\console[colortable02]
Queries value: HKCU\console[colortable03]
Queries value: HKCU\console[colortable04]
Queries value: HKCU\console[colortable05]
Queries value: HKCU\console[colortable06]
Queries value: HKCU\console[colortable07]
Queries value: HKCU\console[colortable08]
Queries value: HKCU\console[colortable09]
Queries value: HKCU\console[colortable10]
Queries value: HKCU\console[colortable11]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[guid]
Queries value: HKCU\console[colortable12]
Queries value: HKCU\console[colortable13]
Queries value: HKCU\console[colortable14]
Queries value: HKCU\console[colortable15]
Queries value: HKCU\console[loadconime]
Queries value: HKCU\console[extendededitkey]
Queries value: HKCU\console[extendededitkeycustom]
Queries value: HKCU\console[worddelimiters]
Queries value: HKCU\console[trimleadingzeros]
Queries value: HKCU\console[enablecolorselection]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data1]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype2]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data2]
Queries value: HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype3]
Queries value: HKCU\console[scrollscale]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype1]

Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ikeext[imagepath]
Queries value: HKLM\system\currentcontrolset\services\ikeext[type]
Queries value: HKLM\system\currentcontrolset\services\ikeext[start]
Queries value: HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ikeext[tag]
Queries value: HKLM\system\currentcontrolset\services\ikeext[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ikeext[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ikeext[group]
Queries value: HKLM\system\currentcontrolset\services\ikeext[objectname]
Queries value: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[action]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[type]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[guid]
Queries value: HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
Queries value:

HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\policyagent[imagepath]
Queries value: HKLM\system\currentcontrolset\services\policyagent[type]
Queries value: HKLM\system\currentcontrolset\services\policyagent[start]
Queries value: HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\policyagent[tag]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\policyagent[group]
Queries value: HKLM\system\currentcontrolset\services\policyagent[objectname]
Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[data0]
Queries value: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[datatype1]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[action]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[type]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[guid]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[datatype0]
Queries value: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[action]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[type]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[data0]
Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[datatype1]
Queries value:

HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype4]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[data0]
Queries value:
HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[type]

Queries value: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\windefend\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[data0]
Queries value: HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1[datatype1]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[data0]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype1]
Queries value: HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[]
Queries value: HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[threadingmodel]
Queries value: HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
Queries value: HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Queries value: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}[]
Queries value: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[]
Queries value: HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\defaulticon[]
Queries value: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}\defaulticon[openicon]
Queries value: HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[localizedstring]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe ui]
Queries value: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}[]
Queries value: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32[]
Queries value: HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}[]
Queries value: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32[]
Queries value: HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations[{57a37caa-367a-4540-916b-f183c5093a4b}]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[zvpebfbsg.jvaqbjf.rkcybere]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32[]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102[checksetting]
Value changes: HKCU\software\microsoft\windows\currentversion\action center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104[checksetting]
Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[librarypath]
  Value changes: HKLM\system\currentcontrolset\services\browser[start]
  Value changes: HKLM\system\currentcontrolset\services\policyagent[start]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[hrzr_pgyfrffvba]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[zvpebfbsg.jvaqbjf.rkcybere]