Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3312, Task ID: 757

Task ID:	757
Risk Level:	10
Date Processed:	2016-05-18 10:34:22 (UTC)
Processing Time:	65.88 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

6	Modifies registry autorun entries
7	Writes to memory of system processes
6	Writes to system32 folder
2	PE: Nonstandard section
5	Abnormal sleep detected
5	Installs service
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
7	Injects thread into Windows process

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\system32\cmd.exe ["C:\Windows\system32\cmd.exe"]
Creates process:	C:\Windows\system32\rundll32.exe [C:\Windows\system32\rundll32.exe bfe.dll,BfeOnServiceStartTypeChange]
Reads from process:	PID:2712 C:\Windows\System32\calc.exe
Writes to process:	PID:1096 C:\Windows\explorer.exe
Writes to process:	PID:436 C:\Windows\System32\services.exe
Writes to process:	PID:2660 C:\Windows\System32\cmd.exe
Terminates process:	C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
Terminates process:	C:\Windows\System32\cmd.exe
Terminates process:	C:\Windows\System32\rundll32.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 mutex:	\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
Creates event:	\BaseNamedObjects\ConsoleEvent-0x00000A6C

File System Events

Creates:	C:\$Recycle.Bin\
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d\L
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d\U
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-1002\$b136cea6dd8900e373425c26f869789d\@
Creates:	C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-

```
1002\$b136cea6dd8900e373425c26f869789d\n
  Creates:                  C:\$Recycle.Bin\S-1-5-18
  Creates:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d
  Creates:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\L
  Creates:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
  Creates:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Creates:                  C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
  Creates:                  C:GAC_MSIL
  Creates:                  C:GAC
  Creates:                  C:\Windows\assembly\GAC\Desktop.ini
  Creates:                  C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
  Opens:                    C:\Windows\Prefetch\859BA9477553CCAD1BBA34C555AB6-401FB0A4.pf
  Opens:                    C:\Windows\System32
  Opens:                    C:\windows\temp\atl.dll
  Opens:                    C:\Windows\System32\atl.dll
  Opens:                    C:\Windows\System32\imm32.dll
  Opens:                    C:\Windows\system32\djusifdsjufkjldsdljkfh
  Opens:                    C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                    C:\Windows\System32\sechost.dll
  Opens:                    C:\windows\temp\Cabinet.dll
  Opens:                    C:\Windows\System32\cabinet.dll
  Opens:                    C:\Windows\System32\mswsock.dll
  Opens:                    C:\Windows\System32\WSHTCPIP.DLL
  Opens:                    C:\windows\temp\CRYPTSP.dll
  Opens:                    C:\Windows\System32\cryptsp.dll
  Opens:                    C:\Windows\System32\rsaenh.dll
  Opens:                    C:\windows\temp\CRYPTBASE.dll
  Opens:                    C:\Windows\System32\cryptbase.dll
  Opens:                    C:\Windows
  Opens:                    C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
  Opens:                    C:\Windows\MSWSOCK.dll
  Opens:                    C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
  Opens:                    C:\Windows\assembly
  Opens:                    C:\Windows\assembly\GAC\Desktop.ini
  Opens:                    C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Opens:                    C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\U
  Opens:                    C:\Windows\System32\cmd.exe
  Opens:                    C:\Windows\System32\apphelp.dll
  Opens:                    C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
  Opens:                    C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Opens:                    C:
  Opens:                    C:\Program Files
  Opens:                    C:\Program Files\Adobe
  Opens:                    C:\Program Files\Adobe\Reader 9.0
  Opens:                    C:\Program Files\Adobe\Reader 9.0\Reader
  Opens:                    C:\Windows\Branding
  Opens:                    C:\Windows\Branding\Basebrd
  Opens:                    C:\Windows\Branding\Basebrd\en-US
  Opens:                    C:\Windows\Globalization
  Opens:                    C:\Windows\Globalization\Sorting
  Opens:                    C:\Windows\System32\en-US
  Opens:                    C:\Windows\System32\ntdll.dll
  Opens:                    C:\Windows\System32\kernel32.dll
  Opens:                    C:\Windows\System32\apisetschema.dll
  Opens:                    C:\Windows\System32\KernelBase.dll
  Opens:                    C:\Windows\System32\locale.nls
  Opens:                    C:\Windows\System32\msvcrt.dll
  Opens:                    C:\Windows\System32\winbrand.dll
  Opens:                    C:\Windows\System32\user32.dll
  Opens:                    C:\Windows\System32\gdi32.dll
  Opens:                    C:\Windows\System32\lpk.dll
  Opens:                    C:\Windows\System32\usp10.dll
  Opens:                    C:\Windows\System32\msctf.dll
  Opens:                    C:\Windows\System32\en-US\cmd.exe.mui
  Opens:                    C:\Windows\Branding\Basebrd\basebrd.dll
  Opens:                    C:\Windows\Branding\Basebrd\en-US\basebrd.dll.mui
  Opens:                    C:\Program Files\Adobe\Reader 9.0\Reader\icucnv36.dll
  Opens:                    C:\Windows\Temp
  Opens:                    C:\Windows\System32\rundll32.exe
  Opens:                    C:\Windows\AppPatch\sysmain.sdb
  Opens:                    C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
  Opens:                    C:\Windows\AppPatch\AcLayers.dll
  Opens:                    C:\Windows\System32\sspicli.dll
  Opens:                    C:\Windows\System32\userenv.dll
  Opens:                    C:\Windows\System32\profapi.dll
  Opens:                    C:\Windows\System32\winspool.drv
  Opens:                    C:\Windows\System32\mpr.dll
  Opens:                    C:\Windows\System32\en-US\rundll32.exe.mui
  Opens:                    C:\Windows\System32\BFE.DLL
  Opens:                    C:\Windows\system32\bfe.dll.manifest
  Opens:                    C:\Windows\system32\bfe.dll.123.Manifest
  Opens:                    C:\Windows\system32\bfe.dll.124.Manifest
  Opens:                C:\Windows\system32\bfe.dll.2.Manifest
  Opens:                C:\Windows\System32\authz.dll
  Opens:                C:\Windows\System32\slc.dll
  Opens:                C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
  Opens:                C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
  Opens:                C:\Windows\System32\calc.exe
  Opens:                C:\
  Writes to:            C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\@
  Writes to:            C:\$Recycle.Bin\S-1-5-21-2160590473-689474908-1361669368-
1002\$b136cea6dd8900e373425c26f869789d\n
  Writes to:            C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Writes to:            C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\n
  Writes to:            C:\Windows\assembly\GAC\Desktop.ini
  Writes to:            C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
  Reads from:           C:\Windows\Prefetch\CMD.EXE-4A81B364.pf
  Reads from:           C:\$Recycle.Bin\S-1-5-18\$b136cea6dd8900e373425c26f869789d\@
  Reads from:           C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
  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:        213.108.252.185:80
  Sends data to:        83.133.123.20:53
  Sends data to:        37.112.0.251:16471
  Sends data to:        68.104.123.244:16471
  Sends data to:        99.225.75.244:16471
  Sends data to:        94.240.212.241:16471
  Sends data to:        111.65.195.241:16471
  Sends data to:        184.66.166.241:16471
  Sends data to:        74.129.114.241:16471
  Sends data to:        70.176.247.237:16471
  Sends data to:        125.4.212.237:16471
  Sends data to:        94.24.192.232:16471
  Sends data to:        182.1.253.230:16471
  Sends data to:        87.3.88.229:16471
  Sends data to:        210.2.239.226:16471
  Sends data to:        71.62.37.224:16471
  Sends data to:        66.158.225.2:16471
  Sends data to:        69.242.115.222:16471
  Sends data to:        178.48.109.222:16471
  Sends data to:        83.14.18.222:16471
  Sends data to:        90.229.137.221:16471
  Sends data to:        219.173.240.2:16471
  Sends data to:        115.38.18.4:16471
  Sends data to:        72.48.52.8:16471
  Sends data to:        68.148.21.218:16471
  Sends data to:        46.237.125.216:16471
  Sends data to:        98.220.121.216:16471
  Sends data to:        89.214.82.216:16471
  Sends data to:        85.230.116.8:16471
  Sends data to:        173.19.154.215:16471
  Sends data to:        206.53.110.9:16471
  Sends data to:        142.167.122.9:16471
  Sends data to:        89.132.206.9:16471
  Sends data to:        75.131.172.213:16471
  Sends data to:        78.23.0.213:16471
  Sends data to:        186.10.14.10:16471
  Sends data to:        76.123.75.212:16471
  Sends data to:        113.211.35.11:16471
  Sends data to:        122.31.235.211:16471
  Sends data to:        46.128.24.13:16471
  Sends data to:        114.74.200.13:16471
  Sends data to:        87.1.83.15:16471
  Sends data to:        138.124.19.16:16471
  Sends data to:        121.84.80.16:16471
  Sends data to:        76.126.235.205:16471
  Sends data to:        69.143.155.205:16471
  Sends data to:        151.33.20.205:16471
  Sends data to:        93.171.119.17:16471
  Sends data to:        89.181.132.204:16471
  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
 Deletes value:           HKLM\software\microsoft\windows\currentversion\run[windows defender]
 Opens key:               HKLM\system\currentcontrolset\control\session manager
 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\policies\microsoft\windows\safer\codeidentifiers
 Opens key:               HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key:               HKCU\
 Opens key:               HKCU\control panel\desktop\muicached\machinelanguageconfiguration
 Opens key:               HKLM\software\policies\microsoft\mui\settings
 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\microsoft\windows\currentversion\sidebyside
 Opens key:               HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key:               HKLM\system\currentcontrolset\control\error message instrument\
 Opens key:               HKLM\system\currentcontrolset\control\error message instrument
 Opens key:               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\
 Opens key:               HKLM\software\microsoft\windows nt\currentversion\windows
 Opens key:               HKLM\system\currentcontrolset\control\nls\customlocale
 Opens key:               HKLM\system\currentcontrolset\control\nls\extendedlocale
 Opens key:               HKLM\software\microsoft\windows nt\currentversion\diagnostics
 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\00000019
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
 Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\0000000c
 Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\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\tcpip6\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\psched\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
  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\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  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\dllnxoptions
  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\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\setup
  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\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\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\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKU\.default\environment
  Opens key:                HKU\.default\volatile environment
  Opens key:                HKU\.default\volatile environment\0
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
  Opens key:                HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\rundll32.exe
  Opens key:                HKU\.default\control
panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                HKU\.default\software\policies\microsoft\control panel\desktop
  Opens key:                HKU\.default\control panel\desktop\languageconfiguration
  Opens key:                HKU\.default\control panel\desktop
  Opens key:                HKU\.default\control panel\desktop\muicached
```

```
 Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key:                HKU\.default\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key:                HKLM\software\microsoft\ole
 Opens key:                HKLM\software\microsoft\ole\tracing
 Opens key:                HKLM\software\microsoft\oleaut
 Opens key:                HKLM\system\currentcontrolset\control\networkprovider\hworder
 Opens key:                HKLM\system\currentcontrolset\services\bfe
 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\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\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\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\clr_optimization_v2.0.50727_32
 Opens key:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32\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\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\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\services\dnscache\triggerinfo\1
 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\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\ehrecvr
 Opens key:                HKLM\system\currentcontrolset\services\ehrecvr\triggerinfo
 Opens key:                HKLM\system\currentcontrolset\services\ehsched
 Opens key:                HKLM\system\currentcontrolset\services\ehsched\triggerinfo
 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\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\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\idsvc
Opens key:                HKLM\system\currentcontrolset\services\idsvc\triggerinfo
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\ipbusenum
Opens key:                HKLM\system\currentcontrolset\services\ipbusenum\triggerinfo
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\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\mcx2svc
Opens key:                HKLM\system\currentcontrolset\services\mcx2svc\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\netlogon
Opens key:                HKLM\system\currentcontrolset\services\netlogon\triggerinfo
Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledsessions\
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\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\power
Opens key:                HKLM\system\currentcontrolset\services\power\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\profsvc
Opens key:                HKLM\system\currentcontrolset\services\profsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\protectedstorage
Opens key:                HKLM\system\currentcontrolset\services\protectedstorage\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\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\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\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\sppuinotify
Opens key:                HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo
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\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\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\tbs
Opens key:               HKLM\system\currentcontrolset\services\tbs\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\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\uxsms
Opens key:               HKLM\system\currentcontrolset\services\uxsms\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\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\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\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\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\wsearch
Opens key:               HKLM\system\currentcontrolset\services\wsearch\triggerinfo
Opens key:               HKLM\system\currentcontrolset\services\wuauserv
Opens key:               HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
```

```
  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\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}\progid
  Opens key:                HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
  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\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\treatas
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\progid
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler32
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprochandler
  Opens key:                HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\treatas
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\progid
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprochandler32
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprochandler
  Opens key:                HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprochandler
  Opens key:                HKCU\software\classes\applications\calc.exe
  Opens key:                HKCR\applications\calc.exe
  Opens key:                HKLM\software\microsoft\ctf\knownclasses
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\treatas
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\progid
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprochandler32
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprochandler
  Opens key:                HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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:            HKCU\control panel\desktop[preferreduilanguages]
  Queries value:            HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[859ba9477553ccad1bba34c555ab6a1b]
  Queries value:            HKLM\software\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\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\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[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\winsock2\parameters[ws2_32spincount]
  Queries value:             HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\psched\parameters\winsock[mapping]
  Queries value:             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\psched[winsock 2.0 provider id]
  Queries value:             HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:             HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:             HKLM\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\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:             HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:             HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  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\image file execution
options\dllnxoptions[usefilter]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[n]
  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\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
  Queries value:             HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:             HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:             HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
  Queries value:             HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
  Queries value:             HKLM\software\microsoft\windows\currentversion[programw6432dir]
  Queries value:             HKLM\software\microsoft\windows\currentversion[commonw6432dir]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\compatibility32[cmd]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
  Queries value:             HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
  Queries value:             HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:             HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Queries value:             HKU\.default\control panel\desktop[preferreduilanguages]
  Queries value:             HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[rundll32]
```

```
  Queries value:          HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:          HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  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\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\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\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
  Queries value:          HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
  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:          HKLM\system\currentcontrolset\services\dnscache[dependongroup]
  Queries value:          HKLM\system\currentcontrolset\services\dnscache[group]
  Queries value:          HKLM\system\currentcontrolset\services\dnscache[objectname]
  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\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\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\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\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
  Queries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
  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\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\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\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\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\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\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\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:              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:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
   Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
   Queries value:              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[threadingmodel]
   Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
   Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[]
   Queries value:              HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[threadingmodel]
   Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[]
   Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
   Queries value:              HKCR\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32[threadingmodel]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-
9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
   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:              HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
   Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
   Value changes:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  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\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[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]
```