Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3312, Task ID: 758

Task ID: 758 Risk Level: 10

Date Processed: 2016-05-18 10:34:35 (UTC)

Processing Time: 63.15 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 Type: PE32:win32:gui File Size: 199680 bytes

MD5: 859ba9477553ccad1bba34c555ab6a1b

SHA256: 339ff6766efd4c5f26a8c0c9413b68ae664bb5eb8dfa403bec5df2909cbb73a1

Description: None

Pattern Matching Results

Writes to memory of system processes

- 6 Modifies registry autorun entries
- 6 Writes to system32 folder
- 2 PE: Nonstandard section
- 3 HTTP connection response code 200 (success)
- 7 Injects thread into Windows process
- 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
- 5 Abnormal sleep detected
- 3 Long sleep detected
- 5 Installs service

Static Events

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

Process/Thread Events

Creates process: C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe

 $["C:\windows\temp\859ba9477553ccad1bba34c555ab6a1b.exe"\]$

Creates process: C:\Windows\system32\rundl132.exe [C:\Windows\system32\rundl132.exe

bfe.dll,BfeOnServiceStartTypeChange]

Creates process: C:\Windows\Sys\W0\64\cmd.exe ["C:\Windows\system32\cmd.exe"]

Reads from process: PID:3052 C:\Windows\SysWOW64\calc.exe
Writes to process: PID:340 C:\Windows\explorer.exe
Writes to process: PID:444 C:\Windows\System32\services.exe
Writes to process: PID:2780 C:\Windows\SysWOW64\cmd.exe

Terminates process: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Terminates process: C:\Windows\SysWOW64\cmd.exe
Terminates process: C:\Windows\System32\rund1132.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\{OC5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
Creates event:	\BaseNamedObjects\ConsoleEvent=0x00000000000AFC

File System Events

Creates: C:\\$Recycle.Bin\

Creates: C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001

Creates: C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2

Creates: C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\L

Creates: C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\U

Creates: C:\\$Recycle.Bin\\$-1-5-21-980053277-1733835069-2361817685-

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\@

Creates: C:\\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-

```
C:\$Recycle.Bin\S-1-5-18
  Creates:
  Creates:
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2
  Creates:
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\L
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
  Creates:
  Creates:
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
  Creates:
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
                                        C:GAC MSIL
  Creates:
  Creates:
                                        C:GAC
                                        C:GAC_32
  Creates:
                                        C:GAC_64
  Creates:
  Creates:
                                        C:\Windows\assembly\GAC_64\Desktop.ini
  Creates:
                                        C:\Windows\assembly\GAC_32\Desktop.ini
                                        C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
  Creates:
  Creates:
                                        C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b
  Creates:
                                        C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
  Opens:
                                        C:\Windows\Prefetch\859BA9477553CCAD1BBA34C555AB6-401FB0A4.pf
  Opens:
                                        C:\Windows
  Opens:
                                        C:\Windows\System32\wow64.dll
  Opens:
                                        C:\Windows\System32\wow64win.dll
  Opens:
                                        C:\Windows\System32\wow64cpu.dll
  Opens:
                                        C:\Windows\system32\wow64log.dll
  Opens:
                                        C:\Windows\SysWOW64
  Opens:
                                        C:\Windows\SysWOW64\sechost.dll
  Opens:
                                        C:\windows\temp\atl.dll
                                        C:\Windows\SysWOW64\atl.dll
  Opens:
  Opens:
                                        C:\Windows\SysWOW64\imm32.dll
  Opens:
                                        C:\Windows\SysWOW64\djusifdsjufkjldsdljkfh
  Opens:
                                        C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:
                                        C:\windows\temp\Cabinet.dll
  Opens:
                                        C:\Windows\SysWOW64\cabinet.dll
  Opens:
                                        C:\Windows\SysWOW64\mswsock.dll
  Opens:
                                        C:\Windows\SysWOW64\WSHTCPIP.DLL
  Opens:
                                        C:\windows\temp\CRYPTSP.dll
                                        C:\Windows\SysWOW64\cryptsp.dll
  Opens:
  Opens:
                                        C:\Windows\SysWOW64\rsaenh.dll
  Opens:
                                        C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
                                        C:\Windows\MSWSOCK.dll
                                        C:\Windows\System32\mswsock.dll
  Opens:
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
  Opens:
  Opens:
                                        C:\Windows\assembly
                                        C:\Windows\assembly\GAC_32\Desktop.ini
  Opens:
                                        C:\Windows\assembly\GAC_64\Desktop.ini
  Opens:
  Opens:
                                        C:\Windows\System32\cryptsp.dll
  Opens:
                                        C:\Windows\System32\rsaenh.dll
                                        \label{lem:c:secycle.Bin\s-1-5-18} C: \short{\$Recycle.Bin\short{\$-1-5-18}} aaa 1415b79b8dbbd8bd16c842c1858a2 \end{2mm} \hfill{\$Recycle.Bin\short{\$-1-5-18}} aaa 1415b79b8dbbd8bd16c842c1858a2 \end{2mm} \hfill{\$Recycle.Bin\short{\$-1-5-18}} \hfill{\$Recycle.Bin\short{\$-1-5-18}} aaa 1415b79b8dbbd8bd16c842c1858a2 \end{2mm} \hfill{\$Recycle.Bin\short{\$-1-5-18}} \hfill{\$-1-5-18} \hfill{\$-1-5-18} aaa 1415b79b8dbbd8bd16c842c1858a2 \end{2mm} \hfill{\$-1-5-18} \hfill{\$-1-5-18} aaa 1415b79b8dbbd8bd16c842c1858a2 \end{2mm} \hfill{\$-1-5-18} \hf
  Opens:
  Opens:
                                        C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
  Opens:
                                        C:\Windows\SvsWOW64\cmd.exe
  Opens:
                                        C:\Windows\Temp
  Opens:
                                        C:\Windows\System32\rundll32.exe
  Opens:
                                        C:\Windows\Prefetch\RUNDLL32.EXE-39102DB5.pf
  Opens:
                                        C:\Windows\System32
  Opens:
                                        C:\Windows\SysWOW64\apphelp.dll
                                        C:\Windows\AppPatch\sysmain.sdb
  Opens:
  Opens:
                                        C:\Windows\SysWOW64\ui\SwDRM.dll
  Opens:
                                        C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe
  Opens:
                                        C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
  Opens:
  Opens:
                                        C:\Windows\SysWOW64\winbrand.dll
  Opens:
                                        C:\Windows\SysWOW64\en-US\cmd.exe.mui
                                        C: \verb|\windows\System32\LogFiles\Scm\d22b06f4-3c25-4d82-b665-f21eb07c8662| \\
  Opens:
                                        C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
  Opens:
1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
                                        C:\Windows\System32\imm32.dll
  Opens:
                                        C:\Windows\System32\en-US\rundll32.exe.mui
  Opens:
  Opens:
                                        C:\Windows\System32\BFE.DLL
  Opens:
                                        C:\Windows\system32\bfe.dll.manifest
  Opens:
                                        C:\Windows\system32\bfe.dll.123.Manifest
                                        C:\Windows\system32\bfe.dll.124.Manifest
  Opens:
  Opens:
                                        C:\Windows\system32\bfe.dll.2.Manifest
  Opens:
                                        C:\Windows\System32\authz.dll
  Opens:
                                        C:\Windows\System32\slc.dll
  Opens:
                                        C:\Windows\System32\sechost.dll
  Opens:
                                        C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b
                                        C: \verb|\windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8|
  Opens:
  Opens:
                                        C:\Windows\System32\LogFiles\Scm\2f57269b-1e09-4e2d-ab1e-b0fdac7d279c
  Opens:
                                        C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
                                        C:\Windows\SysWOW64\calc.exe
  Opens:
  Opens:
                                        C:\Windows\System32\UIAnimation.dll
  Opens:
                                        C:\Users\Admin\Desktop
                                        C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-
  Writes to:
```

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\@

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\n

```
Writes to: C:\$Recycle.Bin\$-1-5-21-980053277-1733835069-2361817685-
```

1001\\$aaa1415b79b8dbbd8bd16c842c1858a2\n

Sends data to:

76.109.133.206:16470

Writes to: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Writes to: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\n

Writes to: C:\Windows\assembly\GAC_64\Desktop.ini
Writes to: C:\Windows\assembly\GAC_32\Desktop.ini

 Writes to:
 C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8

 Writes to:
 C:\Windows\System32\LogFiles\Scm\c016366b-7126-46ca-b36b-592a3d95a60b

 Writes to:
 C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48

Reads from: C:\Windows\SysWOW64\cmd.exe

Reads from: C:\Windows\System32\LogFiles\Scm\d22b06f4-3c25-4d82-b665-f21eb07c8662

Reads from: C:\\$Recycle.Bin\S-1-5-18\\$aaa1415b79b8dbbd8bd16c842c1858a2\@

 $\label{lem:reads} Reads from: $$C:\windows\system32\logFiles\scm\e22a8667-f75b-4ba9-ba46-067ed4429de8$$ Reads from: $$C:\windows\system32\logFiles\scm\c016366b-7126-46ca-b36b-592a3d95a60b$$ Reads from: $$C:\windows\system32\logFiles\scm\2f57269b-1e09-4e2d-ab1e-b0fdac7d279c$$$

Deletes: C:\Windows\Temp\859ba9477553ccad1bba34c555ab6a1b.exe

Network Events DNS query: promos.fling.com promos.fling.com \Rightarrow 208.91.207.58 DNS response: 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: 66.169.64.252:16470 Sends data to: 70.245.30.44:16470 Sends data to: 24.166.74.57:16470 Sends data to: 84.238.123.251:16470 Sends data to: 98.200.159.59:16470 Sends data to: 24.166.102.61:16470 Sends data to: 207.253.171.66:16470 Sends data to: 76.90.0.73:16470 Sends data to: 99.250.124.73:16470 Sends data to: 90.129.15.104:16470 Sends data to: 207.98.234.114:16470 Sends data to: 75.177.68.122:16470 Sends data to: 209.20.29.125:16470 Sends data to: 98.203.59.126:16470 Sends data to: 98.223.143.132:16470 Sends data to: 68.44.66.138:16470 Sends data to: 67.183.232.147:16470 Sends data to: 81.233.194.148:16470 Sends data to: 90.237.150.151:16470 Sends data to: 76.17.49.27:16470 75.71.170.178:16470 Sends data to: Sends data to: 94.191.193.25:16470 Sends data to: 64.244.39.17:16470 Sends data to: 190.172.245.16:16470 Sends data to: 70.66.158.194:16470 Sends data to: 180.215.28.200:16470 Sends data to: 62.143.199.5:16470 Sends data to: 68.35.93.217:16470 Sends data to: 24.7.243.232:16470 Sends data to: 76.84.200.232:16470 Sends data to: 113.211.25.228:16470 Sends data to: 108.162.165.226:16470 Sends data to: 65.26.156.226:16470 184.58.36.223:16470 Sends data to: Sends data to: 202.147.221.2:16470 Sends data to: 83.254.124.221:16470 121.73.119.3:16470 Sends data to: Sends data to: 206.174.8.235:16470 Sends data to: 173.179.2.4:16470 81.233.3.4:16470 Sends data to: Sends data to: 176.198.31.4:16470 Sends data to: 89.239.230.213:16470 Sends data to: 24.252.143.4:16470 189.106.146.212:16470 Sends data to: Sends data to: 24.223.187.210:16470 24.60.167.210:16470 Sends data to: 70.80.21.5:16470 Sends data to: Sends data to: 96.22.40.5:16470 Sends data to: 68.224.54.5:16470 113.35.220.208:16470 Sends data to: Sends data to: 107.9.219.208:16470 Sends data to: 68.59.113.5:16470 Sends data to: 87.50.25.235:16470 Sends data to: 62.75.219.6:16470 Sends data to: 122.132.159.11:16470

Receives data from: 0.0.0.0:0

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

213.108.252.185:80 Receives data from:

Windows Registry Events

HKCU\software\classes\clsid Creates key:

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

options

Opens key: HKLM\system\currentcontrolset\control\session manager

Opens key: HKLM\software\microsoft\wow64

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file

execution options

HKLM\system\currentcontrolset\control\terminal server Opens kev: Opens key: Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key:

HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: Opens key: HKLM\system\currentcontrolset\control\nls\language Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete

Opens kev: HKLM\software\wow6432node\policies\microsoft\mui\settings

Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\

Opens key: $\label{lem:hkcu} \begin{tabular}{ll} HKCU\control\ panel\desktop\muicached\machinelanguageconfiguration \end{tabular}$ Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration

Opens key: HKCU\software\policies\microsoft\control panel\desktop Opens kev: ${\tt HKCU \backslash control\ panel \backslash desktop \backslash language configuration}$

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside Opens kev:

Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\

HKLM\software\wow6432node\microsoft\windows Opens key:

nt\currentversion\diagnostics

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\gre_initialize

Opens key: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime

compatibility

Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens key: HKLM\software\microsoft\sqmclient\windows

 $HKLM \verb|\system| current control set \verb|\services| winsock 2 \verb|\parameters| \\$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\2f2e863f

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

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001 Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

Opens key:

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

Opens key:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000028

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\000000000006

Opens key: HKLM\system\currentcontrolset\services\winsock\parameters
Opens key: HKLM\system\currentcontrolset\services\tcpip6\parameters\winsock
Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters\winsock

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

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

migration\providers\tcpip

Opens key:

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\wow6432node\microsoft\cryptography\offload

Opens key:

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-

9a6f-135d9c6622cc}

Opens key:

 $HKLM \ software \ `microsoft \ `windows \ `current version \ `explorer \ shells er vice objects \ \{f56f6fdd-aa9d-4618-a949-c1b91af43b1a\}$

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

Opens key: HKLM\software\wow6432node\microsoft\rpc

 $Opens\ key: \\ HKLM \ system \ current control set \ control \ computer name \ active computer name$

Opens key: HKLM\system\setup

Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc

Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrol\sqmservicelist

Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32

Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries 64 \000000000010 \parameters \end{substitute} Opens \end{substitute} key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000007
Opens key:

```
cryptographic provider v1.0
```

Opens key: HKLM\software\microsoft\cryptography\offload

Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\software\microsoft\windows nt\currentversion\profilelist
Opens key: HKLM\system\currentcontrol\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: 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: HKLM\software\microsoft\windows\currentversion\sidebyside

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

 $Opens\;key: \\ \qquad \qquad \text{HKLM} software \verb|\wow6432| node \verb|\policies| microsoft \verb|\windows| appcompat| }$

Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: HKLM\software\microsoft\windows

nt\currentversion\appcompatflags\custom\cmd.exe

Opens key: HKLM\system\currentcontrolset\services\aelookupsvc

Opens key: HKLM\system\currentcontrolset\services\alg

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: HKLM\system\currentcontrolset\services\appidsvc
Opens key: HKLM\system\currentcontrolset\services\appinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt

Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder

Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\axinstsv
Opens key: HKLM\system\currentcontrolset\services\bdesvc
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bthserv

Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64

Opens key: HKLM\system\currentcontrolset\services\comsysapp Opens kev: HKLM\system\currentcontrolset\services\cryptsvc Opens key: Opens key: HKLM\system\currentcontrolset\services\defragsvc Opens key: HKLM\system\currentcontrolset\services\dnscache HKLM\system\currentcontrolset\services\dot3svc Opens key: Opens key: HKLM\system\currentcontrolset\services\eaphost Opens key: HKLM\system\currentcontrolset\services\efs ${\it HKLM} \verb|\system| current control set \verb|\services| ehrecvr|\\$ Opens key: Opens key: HKLM\system\currentcontrolset\services\ehsched Opens key: HKLM\system\currentcontrolset\services\eventsystem

Opens key: HKLM\system\currentcontrolset\services\fax
Opens key: HKLM\system\currentcontrolset\services\fdphost
Opens key: HKLM\system\currentcontrolset\services\fdrespub
Opens key: HKLM\system\currentcontrolset\services\fontcache
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0

Opens key: HKLM\system\currentcontrolset\services\hidserv
Opens key: HKLM\system\currentcontrolset\services\hkmsvc

Opens key: HKLM\system\currentcontrolset\services\homegrouplistener
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider

Opens key: HKLM\system\currentcontrolset\services\idsvc Opens key: HKLM\system\currentcontrolset\services\ivmservice Opens key: HKLM\system\currentcontrolset\services\keyiso Opens key: HKLM\system\currentcontrolset\services\ktmrm Opens key: HKLM\system\currentcontrolset\services\lltdsvc Opens key: HKLM\system\currentcontrolset\services\mcx2svc Opens key: HKLM\system\currentcontrolset\services\msdtc Opens key: HKLM\system\currentcontrolset\services\msiscsi Opens kev: HKLM\svstem\currentcontrolset\services\msiserver Opens key: HKLM\system\currentcontrolset\services\napagent

Opens key: HKLM\system\currentcontrolset\services\netlogon

Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing

Opens kev: HKLM\system\currentcontrolset\services\ose HKLM\system\currentcontrolset\services\p2pimsvc Opens key: Opens kev: HKLM\svstem\currentcontrolset\services\p2psvc Opens key: HKLM\system\currentcontrolset\services\peerdistsvc HKLM\system\currentcontrolset\services\perfhost Opens key: Opens key: HKLM\system\currentcontrolset\services\pla Opens key: HKLM\system\currentcontrolset\services\pnrpsvc HKLM\system\currentcontrolset\services\policyagent Opens key: Opens kev: HKLM\svstem\currentcontrolset\services\protectedstorage

Opens key: HKLM\system\currentcontrolset\services\rasauto Opens key: HKLM\system\currentcontrolset\services\rasman HKLM\system\currentcontrolset\services\remoteaccess Opens key: Opens key: HKLM\system\currentcontrolset\services\remoteregistry HKLM\system\currentcontrolset\services\rpceptmapper Opens key: HKLM\system\currentcontrolset\services\rpclocator Opens kev: Opens key: HKLM\system\currentcontrolset\services\samss Opens key: HKLM\system\currentcontrolset\services\scardsvr HKLM\system\currentcontrolset\services\scpolicysvc Opens key: Opens key: HKLM\system\currentcontrolset\services\sdrsvc Opens key: HKLM\system\currentcontrolset\services\seclogon HKLM\system\currentcontrolset\services\sensrsvc Opens kev: Opens key: HKLM\system\currentcontrolset\services\snmptrap Opens key: HKLM\system\currentcontrolset\services\spooler Opens key: HKLM\system\currentcontrolset\services\sppsvc Opens key: HKLM\system\currentcontrolset\services\sppuinotify Opens key: HKLM\system\currentcontrolset\services\ssdpsrv Opens kev: HKLM\svstem\currentcontrolset\services\sstpsvc Opens key: HKLM\system\currentcontrolset\services\stisvc Opens key: HKLM\system\currentcontrolset\services\storsvc HKLM\system\currentcontrolset\services\swprv Opens key:

Opens key: HKLM\system\currentcontrolset\services\sysmain
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice

Opens key: HKLM\system\currentcontrolset\services\tapisrv
Opens key: HKLM\system\currentcontrolset\services\tbs

Opens key: HKLM\system\currentcontrolset\services\threadorder
Opens key: HKLM\system\currentcontrolset\services\tlntsvr

Opens key: HKLM\system\currentcontrolset\services\trustedinstaller
Opens key: HKLM\system\currentcontrolset\services\ui0detect
Opens key: HKLM\system\currentcontrolset\services\upnphost
Opens key: HKLM\system\currentcontrolset\services\vaultsvc
Opens key: HKLM\system\currentcontrolset\services\vaultsvc

Opens key: HKLM\system\currentcontrolset\services\vds
Opens key: HKLM\system\currentcontrolset\services\vds
Opens key: HKLM\system\currentcontrolset\services\wbengine
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc

Opens key: HKLM\system\currentcontrolset\services\webclient
Opens key: HKLM\system\currentcontrolset\services\webclient
Opens key: HKLM\system\currentcontrolset\services\wecsvc
Opens key: HKLM\system\currentcontrolset\services\wercplsupport
Opens key: HKLM\system\currentcontrolset\services\wersvc

Opens key: HKLM\system\currentcontrolset\services\winrm Opens key: HKLM\system\currentcontrolset\services\wlansvc Opens kev: HKLM\system\currentcontrolset\services\wmiapsrv Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc Opens key: HKLM\system\currentcontrolset\services\wpcsvc Opens key: HKLM\system\currentcontrolset\services\wsearch HKLM\system\currentcontrolset\services\wuauserv Opens key: Opens key: HKLM\system\currentcontrolset\services\wudfsvc Opens key: HKLM\system\currentcontrolset\services\wwansvc

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

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

Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
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\triggerinfo
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\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appingmt\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0

```
HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
 Opens key:
                         HKLM\system\currentcontrolset\services\bfe\triggerinfo
 Opens key:
 Opens kev:
                         HKLM\system\currentcontrolset\services\bits\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\browser
 Opens kev:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo
                         HKLM \verb|\system| current control set \verb|\services| browser \verb|\triggerinfo| 0
 Opens key:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\2
 Opens key:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
 Opens kev:
                         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\triggerinfo
 Opens key:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\cscservice
 Opens key:
                         HKLM\system\currentcontrolset\services\cscservice\triggerinfo
                         HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
 Opens kev:
 Opens key:
                         HKLM\system\currentcontrolset\services\dhcp
 Opens key:
                         HKLM\system\currentcontrolset\services\dhcp\triggerinfo
 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
                         HKLM\system\currentcontrolset\services\dot3svc\triggerinfo
 Opens kev:
 Opens key:
                         HKLM\system\currentcontrolset\services\dps
 Opens key:
                         HKLM\system\currentcontrolset\services\dps\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\eaphost\triggerinfo
 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\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\ehsched\triggerinfo
                         HKLM\system\currentcontrolset\services\eventlog
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\eventlog\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\eventsystem\triggerinfo
                         HKLM\system\currentcontrolset\services\fax\triggerinfo
 Opens key:
 Opens key:
                         Opens key:
                         HKLM\system\currentcontrolset\services\fdrespub\triggerinfo
                         HKLM\system\currentcontrolset\services\fontcache\triggerinfo
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\gpsvc
                         HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
                         HKLM \verb|\system| current control set \verb|\services| hidserv \verb|\triggerinfo|| 1
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\idsvc\triggerinfo
 Opens kev:
                         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
                         HKLM\system\currentcontrolset\services\ipbusenum
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\ipbusenum\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\keyiso\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo
 Opens key:
                         Opens key:
                         HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
                         HKLM\system\currentcontrolset\services\lanmanserver
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\lanmanworkstation
                         HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\lmhosts
                         HKLM\system\currentcontrolset\services\lmhosts\triggerinfo
 Opens key:
 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\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\mmcss
                         \label{lem:hklmsystem} \verb+Kklmsystem+ current control set+ services+ \verb+mmcss+ trigger info
 Opens key:
 Opens key:
                         HKLM\system\currentcontrolset\services\msdtc\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\msiserver\triggerinfo
 Opens key:
                         HKLM\system\currentcontrolset\services\napagent\triggerinfo
 Opens kev:
                         HKLM\system\currentcontrolset\services\netlogon\triggerinfo
```

HKLM\software\microsoft\sqmclient\windows\disabledprocesses\

Opens key:

HKLM\software\microsoft\sqmclient\windows\disabledsessions\ Opens key: Opens key: HKLM\system\currentcontrolset\services\netman ${\it HKLM} \verb|\system| current controlset \verb|\services| netman \verb|\triggerinfo| \\$ Opens kev: Opens key: HKLM\system\currentcontrolset\services\netprofm Opens kev: HKLM\system\currentcontrolset\services\netprofm\triggerinfo Opens key: ${\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ nettcpport sharing \verb|\ trigger info$ HKLM\system\currentcontrolset\services\nlasvc Opens key: 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\svstem\currentcontrolset\services\ose\triggerinfo Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo HKLM\system\currentcontrolset\services\pcasvc Opens key: Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\perfhost\triggerinfo Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo Opens key: HKLM\system\currentcontrolset\services\plugplay HKLM\system\currentcontrolset\services\plugplay\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo Opens kev: Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0 Opens key: Opens key: HKLM\system\currentcontrolset\services\power Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo HKLM\system\currentcontrolset\services\profsvc Opens kev: Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo 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\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rasman\triggerinfo Opens key: ${\tt HKLM \ } system \verb|\ current controlset \verb|\ services \verb|\ remoteaccess \verb|\ triggerinfo|$ Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo Opens key: HKLM\system\currentcontrolset\services\rpcss HKLM\system\currentcontrolset\services\rpcss\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo HKLM\system\currentcontrolset\services\schedule Opens key: Opens key: HKLM\system\currentcontrolset\services\schedule\triggerinfo Opens key: HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo Opens key: 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\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 kev: 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\triggerinfo HKLM\system\currentcontrolset\services\spooler\triggerinfo Opens key: Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo Opens key: HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo Opens key: HKLM\system\currentcontrolset\services\stisvc\triggerinfo HKLM\system\currentcontrolset\services\storsvc\triggerinfo Opens key: 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\triggerinfo Opens key: HKLM\system\currentcontrolset\services\sysmain\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo

Opens key: Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1

Opens key: HKLM\system\currentcontrolset\services\tapisrv\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tbs\triggerinfo Opens key: HKLM\system\currentcontrolset\services\termservice

HKLM\system\currentcontrolset\services\termservice\triggerinfo Opens kev:

 ${\it HKLM \ } system \verb| current control set \verb| services \verb| themes \\$ Opens key:

Opens key: HKLM\system\currentcontrolset\services\themes\triggerinfo Opens key: HKLM\system\currentcontrolset\services\threadorder\triggerinfo Opens key: HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\trkwks

Opens kev: HKLM\svstem\currentcontrolset\services\trkwks\triggerinfo

Opens key:

```
HKLM\system\currentcontrolset\services\ui0detect\triggerinfo
    Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\umrdpservice
                                                              Opens kev:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\upnphost\triggerinfo
    Opens kev:
                                                              HKLM\svstem\currentcontrolset\services\uxsms
    Opens key:
                                                              HKLM\system\currentcontrolset\services\uxsms\triggerinfo
                                                              HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
    Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\vds\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\vss\triggerinfo
                                                              HKLM\system\currentcontrolset\services\w32time
    Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\w32time\triggerinfo
    Opens key:
                                                              Opens key:
                                                              HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
                                                              HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
    Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wbengine\triggerinfo
                                                              HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
    Opens kev:
    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
                                                              HKLM\system\currentcontrolset\services\webclient\triggerinfo
    Opens kev:
    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\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wersvc\triggerinfo
    Opens key:
                                                              HKLM\svstem\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\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
                                                              HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
    Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wpdbusenum
                                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
    Opens key:
    Opens key:
                                                              HKLM \verb|\system| current controlset \verb|\services| wpdbusenum \verb|\triggerinfo|| 0
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
                                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
    Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
    Opens key:
                                                              {\tt HKLM \ } system \verb|\ current control set \verb|\ services \verb|\ wsearch \verb|\ triggerinfo|
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
                                                              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
    Opens kev:
                                                              Opens key:
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
    Opens key:
                                                              HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
    Opens key:
                                                              HKCU\software\microsoft\windows\currentversion\explorer\advanced
    Opens key:
                                                              {\tt HKLM \setminus software \setminus microsoft \setminus windows \setminus current version \setminus explorer \setminus advanced}
    Opens kev:
                                                              HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
                                                              HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
    Opens key:
                                                              HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
    Opens key:
355b7f55341b}\treatas
                                                              HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\progid
                                                              HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
    Opens key:
    Opens key:
                                                              \label{local-classes-wow6432} HKCU \software \classes \wow6432 node \clsid \end{660b} 660b \end{660b} -73a9-4b58-8cae-ended \clsid \end{660b} -23a9-4b58-8cae-ended \clsid \clsi
355b7f55341b}
                                                              HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
    Opens key:
    Opens key:
                                                              HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\progid
                                                              HKCR\wow6432 node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\ \ progid
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32
                                                              HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler32
                                                              \label{lem:hkcrclsid} $$ HKCR\clsid_{660b90c8-73a9-4b58-8cae-355b7f55341b} \in \clsid_{660b90c8-73a9-4b58-8cae-355b7f55341b} $$ In prochamble $$ 12.5 \cline{1.00} \cline{1.00
    Opens key:
    Opens key:
                                                              HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler
                                                              \label{local-bound} $HKCR\clsid{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler $$ \clsid{660b90c8-73a9-4b58-8cae-355b7f55341b}\ \clsid{660b90c8-73a9-4b58-8cae-355b7f55341b} \label{local-bound} $$ \clsid{660b90c8-73a9-4b58-8cae-355b7f55341b}\ \clsid{660b90c8-73a9-4b58-8cae-355b7f55341b} \ \clid{660b90c8-73a9-4b58-8cae-355b7f55341b} \ \clid{660b90c8-73a9-4b58-8cae-355b7655341b} \ \clid{660b90c8-73a9-4b58-8cae-355b7655341b} \ \clid{660b90c8-73a9-4b58-8cae-355b7655341b} \ \clid{660b90c8-73a9-4b58-8cae-355b7655341b} \ \clid{660b90c8-73a9-4b58-8cae-355b7655341b} \ \c
    Opens key:
    Opens key:
                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{a2a9545d-a0c2-42b4-9708-a0b2badd77c8\}
    Opens key:
                                                              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
                                                              HKCU \setminus software \setminus classes \setminus clsid \setminus \{a2a9545d - a0c2 - 42b4 - 9708 - a0c2 - 42b4 - a0c2 - 42b4 - a0c2 - a
    Opens key:
a0b2badd77c8}\treatas
                                                              HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
    Opens kev:
    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\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}

 Opens key:
 HKCR\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}

a0b2badd77c8}\progid

Opens key: HKCR\wow6432node\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid

Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-

a0b2badd77c8}\inprocserver32

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\nprocserver32 \end{tabular}$

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

535773d48449}\progid

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449\}\progid} \\$

Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-

535773d48449}

535773d48449}\progid

Opens key: HKCR\wow6432node\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: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}

 Opens key:
 HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}

 Opens key:
 HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}

1a194be3d0b8}\treatas

Opens key: $\begin{tabular}{ll} HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treat as Opens key: \\ HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treat as Opens key: \\ \begin{tabular}{ll} HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treat as Opens key: \\ \begin{tabular}{ll} HCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treat as Opens key: \\ \begin{tabular}{ll} HCU\software\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treat as Opens key: \\ \begin{tabular}{ll} HCU\software\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\treat as Opens key: \\ \begin{tabular}{ll} HCU\software\clsid\cls$

1a194be3d0b8}\progid

Opens key: $\label{lem:hkcrlsid} \begin{tabular}{ll} HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\progid \end{tabular}$

Opens key: HKCU\software\classes\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-

1a194be3d0b8}

 Opens key:
 HKCR\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}

 Opens key:
 HKCU\software\classes\wow6432node\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}

1a194be3d0b8}\progid

 $Opens\;key: \\ \qquad \qquad \mathsf{HKCR} \\ \mathsf{wow} \\ \mathsf{6432} \\ \mathsf{node} \\ \mathsf{clsid} \\ \mathsf{4c1fc63a-695c-47e8-a339-1a194be3d0b8} \\ \mathsf{progid} \\ \mathsf{clsid} \\ \mathsf{dos} \\ \mathsf{do$

Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-

1a194be3d0b8}\inprocserver32

Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprocserver32

Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-

1a194be3d0b8}\inprochandler32

Opens key: HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4c1fc63a-695c-47e8-a339-

1a194be3d0b8}\inprochandler

Opens key: $\label{eq:hkcr} \mbox{HKCR\clsid} $$ \mbox{HKCR\clsid}_{\mbox{4c1fc63a-695c-47e8-a339-1a194be3d0b8} \in \mbox{HKCR\clsid}_{\mbox{hiprochandler}} $$$

Opens key: HKCU\software\classes\

Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}

 Opens key:
 HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}

 Opens key:
 HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768

Odaa792c380e}\treatas

Odaa792c380e}\progid

Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\progid

Opens key: HKCU\software\classes\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-

0daa792c380e}

Opens key: HKCR\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e} Opens key: HKCU\software\classes\wow6432node\clsid\{bfcd4a0c-06b6-4384-b768-

0daa792c380e}\progid

Opens key: HKCR\www6432node\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\progid

Opens key: HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-

Odaa792c380e}\inprocserver32

Opens key: HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprocserver32

```
Opens key:
                         HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-
0daa792c380e}\inprochandler32
 Opens key:
                         HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprochandler32
                         HKCU\software\classes\clsid\{bfcd4a0c-06b6-4384-b768-
 Opens key:
.
0daa792c380e}\inprochandler
 Opens key:
                         HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\\\\) in prochandler
                         HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
 Opens key:
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\treatas
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\treatas
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\progid
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\progid
 Opens key:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}
                         HKCR\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}
 Opens kev:
 Opens key:
                         HKCU\software\classes\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\progid
                         HKCR\wow6432node\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\progid
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\inprocserver32
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprocserver32
 Opens kev:
 Opens key:
                         HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\inprochandler32
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprochandler32
 Opens key:
 Opens key:
                         HKCU\software\classes\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\inprochandler
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprochandler
 Opens kev:
 Queries value:
                         HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
                         HKLM\system\currentcontrolset\control\session
 Queries value:
manager[cwdillegalindllsearch]
 Queries value:
                         HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Oueries value:
                         HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Oueries value:
                         HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value:
                         HKLM\system\currentcontrolset\control\mui\uilanguages\en-
 Queries value:
us[alternatecodepage]
                         HKCU\control panel\desktop[preferreduilanguages]
 Queries value:
                         HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Oueries value:
 Queries value:
HKLM \verb|\software| \verb|\wow6432| node \verb|\microsoft| \verb|\windows \verb|\currentversion| side by side [prefer external manifest]| \\
 Queries value:
                         HKLM\system\currentcontrolset\control\nls\sorting\versions[]
                         HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Oueries value:
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
                         HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[859ba9477553ccad1bba34c555ab6a1b]
                         HKLM\software\wow6432node\microsoft\windows
 Queries value:
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]
 Oueries value:
                         HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Oueries 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:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
 Oueries value:
HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ protocol\_catalog \ entries \ 0000000000003 \ [packed catalog item]
 Queries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000004[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]

Queries value:

Oueries value:

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

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
 Oueries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ catalog_entries \ 0000000000001 \ [enabled] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version] Oueries value:
- $HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000002[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current control set \services \winsock 2 \parameters \namespace_catalog 5 \catalog_entries \namespace_catal$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[providerid]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[version]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \0000000000004 \cite{lemabled} \end{subarray} Queries value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Oueries value:

Oueries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus names pace_catalog \le catalog_entries \setminus 0000000000005 [displaystring]$

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version] Oueries 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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Oueries 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]
Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]

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\tcpip\parameters\winsock[mapping]

Queries value: HKLM\system\currentcontrolset\services\winsock\setup

migration\providers\tcpip[winsock 2.0 provider id]

Queries value:

 $HKLM \setminus system \setminus current control set \setminus services \setminus tcpip \setminus parameters \setminus winsock [minsock addrlength]$

Queries value:

Queries value:

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

Queries value:

HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Oueries value:

VIM) seftware)

Queries value:

 $\label{lem:hklmsoft} HKLM\software\wow6432 node\microsoft\cryptography\defaults\provider\microsoft\ base\ cryptographic\provider\v1.0[image\path]$

Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

Queries value: HKLM\system\currentcontrol\sa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrol\sat{fipsalgorithmpolicy}
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Oueries 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\rpc[maxrpcsize]

Queries value:

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]

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

Queries value: <LM\system\ci</pre>
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
 Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem] Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
 Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
 Oueries value:

Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_\catalog_entries64\000000000005[packedcatalogitem] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem] Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 4 \ 0000000000003 \ [packed catalog item]$ Oueries value:

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ protocol_catalog \ entries \ 4 \ 00000000000002 \ [packed catalog item]$ Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog_\catalog_entries64\000000000001[packedcatalogitem] Oueries value:

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

Oueries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000005[providerid] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid] Queries value:

Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid] Oueries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\00000000001[providerid]

HKLM\software\microsoft\cryptography\defaults\provider\microsoft base Queries value:

cryptographic provider v1.0[type]

HKLM\software\microsoft\cryptography\defaults\provider\microsoft base Queries value:

cryptographic provider v1.0[image path]

HKLM\software\microsoft\windows Oueries value:

nt\currentversion\profilelist[programdata]

Queries value: HKLM\software\microsoft\windows nt\currentversion\profilelist[public] Oueries 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] HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)] Oueries value: Queries value: HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)] Queries value: HKLM\software\microsoft\windows\currentversion[programw6432dir] Oueries value: HKLM\software\microsoft\windows\currentversion[commonw6432dir] Queries value: $HKLM \ \ \, in the constraint of the constrai$

18[profileimagepath]

Queries value: $\label{lem:hkul.default} HKU\. default\software\microsoft\windows\currentversion\explorer\user$

shell folders[appdata]

Oueries value: HKU\.default\software\microsoft\windows\currentversion\explorer\user

shell folders[local appdata]

Oueries value:

HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]

Oueries value:

HKCU\software\microsoft\windows\currentversion\explorer\shell Oueries value: folders[cache]

HKLM\software\microsoft\windows nt\currentversion\image file execution Oueries value: options[disablelocaloverride]

Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[type] Oueries value: HKLM\svstem\currentcontrolset\services\aelookupsvc[start] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc[tag]

Queries value: HKLM\system\currentcontrolset\services\aelookupsyc[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\aelookupsvc[dependongroup] Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[group]

Queries value: HKLM\system\currentcontrolset\services\aelookupsvc[objectname] Oueries value: HKLM\system\currentcontrolset\services\alg[imagepath] HKLM\system\currentcontrolset\services\alg[type] Queries value: Queries value: HKLM\system\currentcontrolset\services\alg[start]

Oueries value: HKLM\system\currentcontrolset\services\alg[errorcontrol] HKLM\system\currentcontrolset\services\alg[tag] Oueries value:

Queries value: HKLM\system\currentcontrolset\services\alg[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\alg[dependongroup] Queries value: HKLM\system\currentcontrolset\services\alg[group] Oueries value: HKU\.default\control panel\desktop[preferreduilanguages]

Queries value: HKU\.default\control

panel\desktop\muicached[machinepreferreduilanguages]

Oueries value: HKLM\system\currentcontrolset\services\alg[objectname] Oueries value: HKLM\system\currentcontrolset\services\appidsvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\appidsvc[type] Oueries value: HKLM\svstem\currentcontrolset\services\appidsvc[start] Queries value: HKLM\system\currentcontrolset\services\appidsvc[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\appidsvc[tag]

Oueries value: HKLM\system\currentcontrolset\services\appidsvc[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\appidsvc[dependongroup] Queries value: HKLM\system\currentcontrolset\services\appidsvc[group] Oueries value: HKLM\system\currentcontrolset\services\appidsvc[objectname] Queries value: HKLM\system\currentcontrolset\services\appinfo[imagepath]

```
Oueries value:
                          HKLM\system\currentcontrolset\services\appinfo[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appinfo[start]
                          HKLM\system\currentcontrolset\services\appinfo[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\appinfo[tag]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\appinfo[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\appinfo[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appinfo[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appinfo[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appmgmt[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appmgmt[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appmgmt[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\appmgmt[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appmgmt[tag]
                          {\tt HKLM \ } system \verb| current control set \verb| services \verb| appmgmt[dependon service]|
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\appmgmt[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\appmgmt[group]
                          HKLM\system\currentcontrolset\services\appmgmt[objectname]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\audioendpointbuilder[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\audioendpointbuilder[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\audioendpointbuilder[start]
 Oueries value:
HKLM\system\currentcontrolset\services\audioendpointbuilder[errorcontrol]
                          \label{lem:hklm} \verb+Kklm \system \current control set \services \audio endpoint builder [tag]
 Oueries value:
 Queries value:
HKLM\system\currentcontrolset\services\audioendpointbuilder[dependonservice]
 Queries value:
HKLM\system\currentcontrolset\services\audioendpointbuilder[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\audioendpointbuilder[group]
 Queries value:
                          HKLM\svstem\currentcontrolset\services\audioendpointbuilder[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\audiosrv[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\audiosrv[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\audiosrv[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\audiosrv[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\audiosrv[tag]
                          HKLM\system\currentcontrolset\services\audiosrv[dependonservice]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\audiosrv[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\audiosrv[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\audiosrv[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\axinstsv[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\axinstsv[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\axinstsv[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\axinstsv[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\axinstsv[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\axinstsv[dependonservice]
                          HKLM\system\currentcontrolset\services\axinstsv[dependongroup]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\axinstsv[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\axinstsv[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\bdesvc[imagepath]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\bdesvc[tvpe]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bdesvc[start]
                          HKLM\system\currentcontrolset\services\bdesvc[errorcontrol]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\bdesvc[tag]
                          HKLM\software\wow6432node\microsoft\windows
 Oueries value:
nt\currentversion\compatibility32[cmd]
 Oueries value:
                          HKLM\system\currentcontrolset\control\cmf\config[system]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bdesvc[dependonservice]
                          HKLM\system\currentcontrolset\services\bdesvc[dependongroup]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\bdesvc[group]
                          {\tt HKLM \ } system \verb| current control set \verb| services \verb| bdesvc[object name] \\
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\bfe[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\bfe[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\bfe[start]
                          HKLM\system\currentcontrolset\services\bfe[errorcontrol]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\bfe[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bfe[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\bfe[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\bfe[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bfe[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\bits[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\bits[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bits[start]
                          HKLM\system\currentcontrolset\services\bits[errorcontrol]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\bits[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bits[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\bits[dependongroup]
 Queries value:
                          HKLM\svstem\currentcontrolset\services\bits[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bits[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\bthserv[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[tag]
```

HKLM\system\currentcontrolset\services\bthserv[dependonservice]

Queries value:

```
Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\bthserv[objectname]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[imagepath]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[type]
 Oueries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[start]
 Oueries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[errorcontrol]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[tag]
 Oueries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[dependonservice]
 Oueries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[dependongroup]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[group]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32[objectname]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus clr\_optimization\_v2.0.50727\_64 [image path]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[type]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus clr\_optimization\_v2.0.50727\_64[start]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus clr\_optimization\_v2.0.50727\_64[error control]
 Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[tag]
 Queries value:
Queries value:
Queries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[group]
 Oueries value:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64[objectname]
                         HKLM\system\currentcontrolset\services\comsysapp[imagepath]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\comsysapp[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\comsysapp[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\comsysapp[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\comsysapp[tag]
                          HKLM\system\currentcontrolset\services\comsysapp[dependonservice]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\comsysapp[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\comsysapp[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\comsysapp[objectname]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\crvptsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[type]
                          HKLM\system\currentcontrolset\services\cryptsvc[start]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[tag]
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\cryptsvc[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[tag]
                          HKLM\system\currentcontrolset\services\dcomlaunch[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[dependongroup]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\defragsvc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\defragsvc[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\defragsvc[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\defragsvc[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\defragsvc[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\defragsvc[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\defragsvc[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\defragsvc[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\defragsvc[objectname]
 Queries value:
                          HKLM\svstem\currentcontrolset\services\dnscachefimagepathl
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[tag]
 Queries value:
                          HKLM\system\currentcontrolset\services\dnscache[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\dnscache[dependongroup]
```

HKLM\system\currentcontrolset\services\dnscache[group]

Queries value:

Oueries value: HKLM\system\currentcontrolset\services\dnscache[objectname] Oueries value: HKLM\system\currentcontrolset\services\dot3syc[imagepath] Queries value: HKLM\system\currentcontrolset\services\dot3svc[type] Queries value: HKLM\system\currentcontrolset\services\dot3svc[start] Oueries value: HKLM\system\currentcontrolset\services\dot3svc[errorcontrol1 Queries value: HKLM\system\currentcontrolset\services\dot3svc[tag] Oueries value: HKLM\system\currentcontrolset\services\dot3svc[dependonservice] HKLM\system\currentcontrolset\services\dot3svc[dependongroup] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\dot3svc[group] Oueries value: HKLM\system\currentcontrolset\services\dot3svc[objectname] Oueries value: HKLM\system\currentcontrolset\services\eaphost[imagepath] Queries value: HKLM\system\currentcontrolset\services\eaphost[type] Oueries value: HKLM\system\currentcontrolset\services\eaphost[start] Oueries value: HKLM\system\currentcontrolset\services\eaphost[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\eaphost[tag] Oueries value: HKLM\system\currentcontrolset\services\eaphost[dependonservice] Queries value: HKLM\svstem\currentcontrolset\services\eaphost[dependongroup] Queries value: HKLM\system\currentcontrolset\services\eaphost[group] Oueries value: HKLM\system\currentcontrolset\services\eaphost[objectname] Oueries value: HKLM\system\currentcontrolset\services\efs[imagepath] Queries value: HKLM\system\currentcontrolset\services\efs[type] Queries value: HKLM\system\currentcontrolset\services\efs[start] Queries value: HKLM\svstem\currentcontrolset\services\efs[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\efs[tag] Oueries value: HKLM\system\currentcontrolset\services\efs[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\efs[dependongroup] Queries value: HKLM\system\currentcontrolset\services\efs[group] Queries value: HKLM\system\currentcontrolset\services\efs[objectname] HKLM\system\currentcontrolset\services\ehrecvr[imagepath] Queries value: Queries value: HKLM\system\currentcontrolset\services\ehrecvr[type] Queries value: HKLM\system\currentcontrolset\services\ehrecvr[start] Oueries value: HKLM\system\currentcontrolset\services\ehrecvr[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\ehrecvr[tag] Queries value: HKLM\system\currentcontrolset\services\ehrecvr[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\ehrecvr[dependongroup] Queries value: HKLM\system\currentcontrolset\services\ehrecvr[group] Queries value: HKLM\system\currentcontrolset\services\ehrecvr[objectname] Oueries value: HKLM\system\currentcontrolset\services\ehsched[imagepath] Queries value: HKLM\system\currentcontrolset\services\ehsched[type] Queries value: HKLM\system\currentcontrolset\services\ehsched[start] Oueries value: HKLM\system\currentcontrolset\services\ehsched[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\ehsched[tag] Queries value: HKLM\svstem\currentcontrolset\services\ehsched[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\ehsched[dependongroup] HKLM\system\currentcontrolset\services\ehsched[group] Oueries value: Queries value: HKLM\system\currentcontrolset\services\ehsched[objectname] Oueries value: HKLM\system\currentcontrolset\services\eventsystem[imagepath] Queries value: HKLM\system\currentcontrolset\services\eventsystem[type] Oueries value: HKLM\svstem\currentcontrolset\services\eventsvstem[start] Oueries value: HKLM\system\currentcontrolset\services\eventsystem[errorcontrol] HKLM\system\currentcontrolset\services\eventsystem[tag] Oueries value: Queries value: HKLM\system\currentcontrolset\services\eventsystem[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\eventsystem[dependongroup] Queries value: HKLM\system\currentcontrolset\services\eventsystem[group] Oueries value: HKLM\system\currentcontrolset\services\eventsystem[objectname] Queries value: HKLM\system\currentcontrolset\services\fax[imagepath] HKLM\system\currentcontrolset\services\fax[type] Oueries value: HKLM\system\currentcontrolset\services\fax[start] Oueries value: HKLM\system\currentcontrolset\services\fax[errorcontrol] Oueries value: Queries value: HKLM\system\currentcontrolset\services\fax[tag] Queries value: HKLM\system\currentcontrolset\services\fax[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\fax[dependongroup] HKLM\system\currentcontrolset\services\fax[group] Queries value: Queries value: HKLM\system\currentcontrolset\services\fax[objectname] Oueries value: HKLM\system\currentcontrolset\services\fdphost[imagepath] HKLM\system\currentcontrolset\services\fdphost[type] Oueries value: Queries value: HKLM\system\currentcontrolset\services\fdphost[start] Oueries value: HKLM\system\currentcontrolset\services\fdphost[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\fdphost[tag] Queries value: HKLM\system\currentcontrolset\services\fdphost[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\fdphost[dependongroup] HKLM\system\currentcontrolset\services\fdphost[group] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\fdphost[objectname] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[imagepath] Queries value: HKLM\system\currentcontrolset\services\fdrespub[type] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[start] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[tag] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[dependongroup] Queries value: HKLM\system\currentcontrolset\services\fdrespub[group] Oueries value: HKLM\system\currentcontrolset\services\fdrespub[objectname] Queries value: HKLM\system\currentcontrolset\services\fontcache[imagepath]

```
Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\fontcache[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\fontcache[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\fontcache[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[tag]
                          HKLM \setminus system \setminus current control set \setminus services \setminus font cache 3.0.0.0 [depend on service]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\fontcache3.0.0.0[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\hidserv[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv[tag]
                          HKLM\system\currentcontrolset\services\hidserv[dependonservice]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\hidserv[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[type]
 Queries value:
                          HKLM\svstem\currentcontrolset\services\hkmsvc[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\hkmsvc[group]
                          HKLM\system\currentcontrolset\services\hkmsvc[objectname]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[tag]
 Oueries value:
HKLM\system\currentcontrolset\services\homegrouplistener[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[dependongroup]
                          HKLM\system\currentcontrolset\services\homegrouplistener[group]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\homegrouplistener[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\homegroupprovider[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\homegroupprovider[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\homegroupprovider[start]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\homegroupprovider[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\homegroupprovider[tag]
 Oueries value:
HKLM\system\currentcontrolset\services\homegroupprovider[dependonservice]
                          {\tt HKLM \ } system \verb| current control set \verb| services \verb| homegroupprovider [dependon group] \\
 Oueries value:
                          HKLM\system\currentcontrolset\services\homegroupprovider[group]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\homegroupprovider[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\idsvc[imagepath]
                          HKLM\system\currentcontrolset\services\idsvc[type]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\idsvc[start]
                          HKLM\system\currentcontrolset\services\idsvc[errorcontrol]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\idsvc[tag]
 Queries value:
                          HKLM\system\currentcontrolset\services\idsvc[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\idsvc[dependongroup]
                          HKLM\system\currentcontrolset\services\idsvc[group]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\idsvc[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\keyiso[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\keyiso[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\keyiso[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\keyiso[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\keyiso[tag]
 Queries value:
                          HKLM\system\currentcontrolset\services\keyiso[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\keyiso[dependongroup]
                          HKLM\system\currentcontrolset\services\keyiso[group]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\keviso[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\ktmrm[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\ktmrm[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\ktmrm[group]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\ktmrm[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[imagepath]
```

```
Oueries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[start]
                          HKLM\system\currentcontrolset\services\lltdsvc[errorcontrol]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[tag]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\lltdsvc[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lltdsvc[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[type]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\mcx2svc[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[tag]
                          HKLM\system\currentcontrolset\services\mcx2svc[dependonservice]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\mcx2svc[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\msdtc[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msdtc[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msdtc[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msdtc[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msdtc[tag]
                          HKLM\system\currentcontrolset\services\msdtc[dependonservice]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\msdtc[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msdtc[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msdtc[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsi[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsi[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsifstart1
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsi[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsi[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msiscsi[dependonservice]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsi[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiscsi[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msiscsi[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiserver[imagepath]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiserver[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msiserver[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiserver[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiserver[tag]
                          HKLM\system\currentcontrolset\services\msiserver[dependonservice]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\msiserver[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\msiserver[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\msiserver[objectname]
                          HKLM\system\currentcontrolset\services\napagent[imagepath]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\napagent[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\napagent[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\napagent[errorcontrol]
 Oueries value:
                          HKLM\system\currentcontrolset\services\napagent[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\napagent[dependonservice]
                          HKLM\system\currentcontrolset\services\napagent[dependongroup]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\napagent[group]
 Oueries value:
                          HKLM\system\currentcontrolset\services\napagent[objectname]
                          HKLM\system\currentcontrolset\services\netlogon[imagepath]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\netlogon[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\netlogon[start]
                          HKLM\system\currentcontrolset\services\netlogon[errorcontrol]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\netlogon[tag]
                          HKLM \verb|\system| current controlset \verb|\services| netlogon[dependonservice]
 Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\netlogon[dependongroup]
 Queries value:
                          HKLM\system\currentcontrolset\services\netlogon[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\netlogon[objectname]
                          HKLM\system\currentcontrolset\services\nettcpportsharing[imagepath]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\nettcpportsharing[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\nettcpportsharing[start]
 Queries value:
                          HKLM\system\currentcontrolset\services\nettcpportsharing[errorcontrol]
 Queries value:
                          HKLM\system\currentcontrolset\services\nettcpportsharing[tag]
 Oueries value:
HKLM\system\currentcontrolset\services\nettcpportsharing[dependonservice]
                          HKLM\system\currentcontrolset\services\nettcpportsharing[dependongroup]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\nettcpportsharing[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\nettcpportsharing[objectname]
 Queries value:
                          HKLM\system\currentcontrolset\services\ose[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ose[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\ose[start]
                          HKLM\system\currentcontrolset\services\ose[errorcontrol]
 Queries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\ose[tag]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ose[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ose[dependongroup]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ose[group]
 Queries value:
                          HKLM\system\currentcontrolset\services\ose[objectname]
 Oueries value:
                          HKLM\system\currentcontrolset\services\p2pimsvc[imagepath]
```

HKLM\system\currentcontrolset\services\p2pimsvc[type]

Queries value:

```
Oueries value:
                        HKLM\system\currentcontrolset\services\p2pimsvc[start]
                        HKLM\system\currentcontrolset\services\p2pimsvc[errorcontrol]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\p2pimsvc[tag]
                        HKLM\system\currentcontrolset\services\p2pimsvc[dependonservice]
Queries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\p2pimsvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\p2pimsvc[group]
                        HKLM\system\currentcontrolset\services\p2pimsvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[imagepath]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\p2psvc[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\p2psvc[objectname]
Queries value:
                        HKLM\svstem\currentcontrolset\services\peerdistsvc[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\peerdistsvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\perfhost[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\perfhost[type]
Queries value:
                        HKLM\system\currentcontrolset\services\perfhost[start]
                        {\tt HKLM} \verb| system| current control set| services| perfhost[error control]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\perfhost[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\perfhost[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\perfhost[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\perfhost[group]
Queries value:
                        HKLM\system\currentcontrolset\services\perfhost[objectname]
                        HKLM\system\currentcontrolset\services\pla[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\pla[type]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\pla[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\pla[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\pla[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\pla[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\pla[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\pla[group]
Queries value:
                        HKLM\system\currentcontrolset\services\pla[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[imagepath]
                        HKLM\system\currentcontrolset\services\pnrpsvc[type]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[dependongroup]
                        HKLM\system\currentcontrolset\services\pnrpsvc[group]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\pnrpsvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\policyagent[imagepath]
                        HKLM\system\currentcontrolset\services\policyagent[type]
Queries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\policyagent[start]
Queries value:
                        HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
                        HKLM\system\currentcontrolset\services\policyagent[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\policyagent[dependonservice]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\policyagent[dependongroup]
                        HKLM\system\currentcontrolset\services\policyagent[group]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\policyagent[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\protectedstorage[imagepath]
                        HKLM\system\currentcontrolset\services\protectedstorage[type]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\protectedstorage[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\protectedstorage[errorcontrol]
                        HKLM\system\currentcontrolset\services\protectedstorage[tag]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\protectedstorage[dependonservice]
Oueries value:
                        {\tt HKLM \ } system \verb| current control set \verb| services \verb| protected storage[dependon group]|
Queries value:
                        {\it HKLM \ } system \verb| current control set \verb| services \verb| protected storage[group]|
Queries value:
                        HKLM\system\currentcontrolset\services\protectedstorage[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\rasauto[imagepath]
                        HKLM\system\currentcontrolset\services\rasauto[type]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\rasauto[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\rasauto[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\rasauto[tag]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\rasauto[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\rasauto[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\rasauto[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\rasauto[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\rasman[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\rasman[type]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\rasman[start]
Queries value:
                        HKLM\system\currentcontrolset\services\rasman[errorcontrol]
```

```
Oueries value:
                        HKLM\system\currentcontrolset\services\rasman[tag]
                        HKLM\system\currentcontrolset\services\rasman[dependonservice]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\rasman[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\rasman[group]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\rasman[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteaccess[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteregistry[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteregistry[type]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\remoteregistrv[start]
Queries value:
                        HKLM\system\currentcontrolset\services\remoteregistry[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteregistry[tag]
                        {\tt HKLM \setminus system \setminus current control set \setminus services \setminus remote registry [dependon service]}
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteregistry[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\remoteregistry[group]
Queries value:
                        HKLM\system\currentcontrolset\services\remoteregistrv[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[start]
Queries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\rpclocator[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\rpclocator[type]
                        HKLM\system\currentcontrolset\services\rpclocator[start]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\rpclocator[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\rpclocator[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\rpclocator[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\rpclocator[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\rpclocator[group]
                        HKLM\system\currentcontrolset\services\rpclocator[objectname]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\samss[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\samss[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\samss[start]
                        HKLM\system\currentcontrolset\services\samss[errorcontrol]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\samss[tag]
                        {\tt HKLM \ } system \verb| current control set \verb| services \verb| samss[dependon service]|
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\samss[dependongroup]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\samss[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\samss[objectname]
                        HKLM\system\currentcontrolset\services\scardsvr[imagepath]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\scardsyr[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\scardsvr[start]
Queries value:
                        HKLM\system\currentcontrolset\services\scardsvr[errorcontrol]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\scardsvr[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\scardsvr[dependonservice]
                        HKLM\system\currentcontrolset\services\scardsvr[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\scardsvr[group]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\scardsvr[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[type]
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[start]
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[tag]
                        HKLM\system\currentcontrolset\services\scpolicysvc[dependonservice]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\scpolicysvc[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[start]
                        HKLM\system\currentcontrolset\services\sdrsvc[errorcontrol]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\sdrsvc[objectname]
                        HKLM\system\currentcontrolset\services\seclogon[imagepath]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\seclogon[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\seclogon[start]
Queries value:
                        HKLM\system\currentcontrolset\services\seclogon[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\seclogon[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\seclogon[dependonservice]
```

```
Oueries value:
                        HKLM\system\currentcontrolset\services\seclogon[dependongroup]
                        HKLM\system\currentcontrolset\services\seclogon[group]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\seclogon[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[type]
Queries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[group]
Queries value:
                        HKLM\system\currentcontrolset\services\sensrsvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\snmptrap[imagepath]
                        HKLM\system\currentcontrolset\services\snmptrap[type]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\snmptrap[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\snmptrap[errorcontrol]
                        HKLM\svstem\currentcontrolset\services\snmptrap[tag]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\snmptrap[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\snmptrap[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\snmptrap[group]
Queries value:
                        HKLM\system\currentcontrolset\services\snmptrap[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[type]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\spooler[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\spooler[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[group]
Queries value:
                        HKLM\system\currentcontrolset\services\spooler[objectname]
Queries value:
                        HKLM\system\currentcontrolset\services\sppsvc[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\sppsvc[type]
                        HKLM\system\currentcontrolset\services\sppsvc[start]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\sppsvc[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\sppsvc[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\sppsvc[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\sppsvc[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\sppsvc[group]
                        HKLM\system\currentcontrolset\services\sppsvc[objectname]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\sppuinotify[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\sppuinotify[type]
                        {\tt HKLM} \\ system \\ \verb|currentcontrolset| services \\ \\ sppuinotify[start]
Queries value:
Oueries value:
                        HKLM\svstem\currentcontrolset\services\sppuinotifv[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\sppuinotify[tag]
                        HKLM\system\currentcontrolset\services\sppuinotify[dependonservice]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\sppuinotify[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\sppuinotify[group]
Queries value:
                        HKLM\system\currentcontrolset\services\sppuinotify[objectname]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\ssdpsrv[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[type]
                        HKLM\system\currentcontrolset\services\ssdpsrv[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[errorcontrol]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
                        HKLM\system\currentcontrolset\services\sstpsvc[imagepath]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\sstpsvc[type]
                        HKLM\system\currentcontrolset\services\sstpsvc[start]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\sstpsvc[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\sstpsvc[tag]
                        HKLM\system\currentcontrolset\services\sstpsvc[dependonservice]
Queries value:
                        HKLM\system\currentcontrolset\services\sstpsvc[dependongroup]
Queries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\sstpsvc[group]
                        HKLM\system\currentcontrolset\services\sstpsvc[objectname]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\stisvc[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\stisvc[type]
Queries value:
                        HKLM\system\currentcontrolset\services\stisvc[start]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\stisvc[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\stisvc[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\stisvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\stisvc[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\stisvc[group]
Queries value:
                        HKLM\system\currentcontrolset\services\stisvc[objectname]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\storsvc[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\storsvc[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\storsvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\storsvc[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\storsvc[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\storsvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\storsvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\storsvc[group]
```

Oueries value: HKLM\system\currentcontrolset\services\storsvc[objectname] Oueries value: HKLM\system\currentcontrolset\services\swprv[imagepath] Queries value: HKLM\system\currentcontrolset\services\swprv[type] HKLM\system\currentcontrolset\services\swprv[start] Queries value: Oueries value: HKLM\system\currentcontrolset\services\swprv[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\swprv[tag] Oueries value: HKLM\system\currentcontrolset\services\swprv[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\swprv[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\swprv[group] Oueries value: HKLM\system\currentcontrolset\services\swprv[objectname] Oueries value: HKLM\system\currentcontrolset\services\sysmain[imagepath] Queries value: HKLM\system\currentcontrolset\services\sysmain[type] Oueries value: HKLM\system\currentcontrolset\services\sysmain[start] Oueries value: HKLM\system\currentcontrolset\services\sysmain[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\sysmain[tag] Oueries value: HKLM\system\currentcontrolset\services\sysmain[dependonservice] Oueries value: HKLM\svstem\currentcontrolset\services\svsmain[dependongroup] Queries value: HKLM\system\currentcontrolset\services\sysmain[group] Oueries value: HKLM\system\currentcontrolset\services\sysmain[objectname] Oueries value: HKLM\system\currentcontrolset\services\tabletinputservice[imagepath] Oueries value: HKLM\system\currentcontrolset\services\tabletinputservice[type] Oueries value: HKLM\system\currentcontrolset\services\tabletinputservice[start] HKLM\system\currentcontrolset\services\tabletinputservice[errorcontrol] Queries value: Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[tag] Oueries value: $\label{thm:local_equation} \begin{tabular}{ll} HKLM \end{tabular} system \end{tabular} current control set \end{tabular} set \end{tabular} is a like the label through through the label throu$ Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[dependongroup] Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[group] Queries value: HKLM\system\currentcontrolset\services\tabletinputservice[objectname] Queries value: HKLM\system\currentcontrolset\services\tapisrv[imagepath] Queries value: HKLM\system\currentcontrolset\services\tapisrv[type] Oueries value: HKLM\system\currentcontrolset\services\tapisrv[start] Queries value: HKLM\system\currentcontrolset\services\tapisrv[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\tapisrv[tag] HKLM\system\currentcontrolset\services\tapisrv[dependonservice] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tapisrv[dependongroup] Queries value: HKLM\system\currentcontrolset\services\tapisrv[group] Oueries value: HKLM\system\currentcontrolset\services\tapisrv[objectname] Queries value: HKLM\system\currentcontrolset\services\tbs[imagepath] Queries value: HKLM\system\currentcontrolset\services\tbs[type] Queries value: HKLM\system\currentcontrolset\services\tbs[start] Queries value: HKLM\system\currentcontrolset\services\tbs[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\tbs[tag] Oueries value: HKLM\system\currentcontrolset\services\tbs[dependonservice] HKLM\system\currentcontrolset\services\tbs[dependongroup] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tbs[group] Oueries value: HKLM\system\currentcontrolset\services\tbs[objectname] Queries value: HKLM\system\currentcontrolset\services\threadorder[imagepath] Oueries value: HKLM\svstem\currentcontrolset\services\threadorder[tvpe] Oueries value: HKLM\system\currentcontrolset\services\threadorder[start] HKLM\system\currentcontrolset\services\threadorder[errorcontrol] Oueries value: Queries value: HKLM\system\currentcontrolset\services\threadorder[tag] ${\tt HKLM \ } system \verb| current control set \verb| services \verb| thread order [depend on service] \\$ Oueries value: Queries value: HKLM\system\currentcontrolset\services\threadorder[dependongroup] Oueries value: HKLM\svstem\currentcontrolset\services\threadorder[group] Oueries value: HKLM\system\currentcontrolset\services\threadorder[objectname] HKLM\system\currentcontrolset\services\tlntsvr[imagepath] Oueries value: Queries value: HKLM\system\currentcontrolset\services\tlntsvr[type] Oueries value: HKLM\system\currentcontrolset\services\tlntsvr[start] Queries value: HKLM\system\currentcontrolset\services\tlntsvr[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\tlntsvr[tag] Queries value: HKLM\system\currentcontrolset\services\tlntsvr[dependonservice] HKLM\system\currentcontrolset\services\tlntsvr[dependongroup] Queries value: Queries value: HKLM\system\currentcontrolset\services\tlntsvr[group] HKLM\system\currentcontrolset\services\tlntsvr[objectname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[imagepath] Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[type] Oueries value: HKLM\system\currentcontrolset\services\trustedinstaller[start] Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[tag] ${\tt HKLM \ } system \verb|\ 'current controlset \ 'services \ 'trusted in staller [dependon service]$ Oueries value: HKLM\system\currentcontrolset\services\trustedinstaller[dependongroup] Oueries value: Queries value: HKLM\system\currentcontrolset\services\trustedinstaller[group] Oueries value: HKLM\system\currentcontrolset\services\trustedinstaller[objectname] Queries value: HKLM\system\currentcontrolset\services\ui0detect[imagepath] Queries value: HKLM\system\currentcontrolset\services\ui0detect[type] Oueries value: HKLM\system\currentcontrolset\services\ui0detect[start] Oueries value: HKLM\system\currentcontrolset\services\ui0detect[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\ui0detect[tag] Oueries value: HKLM\system\currentcontrolset\services\ui0detect[dependonservice] Queries value: HKLM\system\currentcontrolset\services\ui0detect[dependongroup] Oueries value: HKLM\svstem\currentcontrolset\services\ui0detect[group] Queries value: HKLM\system\currentcontrolset\services\ui0detect[objectname]

Oueries value: HKLM\system\currentcontrolset\services\upnphost[imagepath] Oueries value: HKLM\system\currentcontrolset\services\upnphost[type] Queries value: HKLM\system\currentcontrolset\services\upnphost[start] Queries value: HKLM\system\currentcontrolset\services\upnphost[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\upnphost[tag] Queries value: HKLM\system\currentcontrolset\services\upnphost[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\upnphost[dependongroup] HKLM\system\currentcontrolset\services\upnphost[group] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\upnphost[objectname] Oueries value: HKLM\system\currentcontrolset\services\vaultsvc[imagepath] Oueries value: HKLM\system\currentcontrolset\services\vaultsvc[type] Queries value: HKLM\system\currentcontrolset\services\vaultsvc[start] Oueries value: HKLM\system\currentcontrolset\services\vaultsvc[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\vaultsvc[tag] Oueries value: HKLM\system\currentcontrolset\services\vaultsvc[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\vaultsvc[dependongroup] HKLM\system\currentcontrolset\services\vaultsvc[group] Queries value: Queries value: HKLM\system\currentcontrolset\services\vaultsvc[objectname] Oueries value: HKLM\system\currentcontrolset\services\vds[imagepath] Oueries value: HKLM\system\currentcontrolset\services\vds[type] Queries value: HKLM\system\currentcontrolset\services\vds[start] Oueries value: HKLM\system\currentcontrolset\services\vds[errorcontrol] Queries value: HKLM\svstem\currentcontrolset\services\vds[tag] Queries value: HKLM\system\currentcontrolset\services\vds[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\vds[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\vds[group] Queries value: HKLM\system\currentcontrolset\services\vds[objectname] Queries value: HKLM\system\currentcontrolset\services\vss[imagepath] Queries value: HKLM\svstem\currentcontrolset\services\vss[tvpe] Queries value: HKLM\system\currentcontrolset\services\vss[start] Queries value: HKLM\system\currentcontrolset\services\vss[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\vss[tag] Queries value: HKLM\system\currentcontrolset\services\vss[dependonservice] Queries value: HKLM\system\currentcontrolset\services\vss[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\vss[group] Queries value: HKLM\system\currentcontrolset\services\vss[objectname] Queries value: HKLM\system\currentcontrolset\services\wbengine[imagepath] Oueries value: HKLM\system\currentcontrolset\services\wbengine[type] Queries value: HKLM\system\currentcontrolset\services\wbengine[start] Queries value: HKLM\system\currentcontrolset\services\wbengine[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\wbengine[tag] Queries value: HKLM\system\currentcontrolset\services\wbengine[dependonservice] Queries value: HKLM\system\currentcontrolset\services\wbengine[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\wbengine[group] HKLM\system\currentcontrolset\services\wbengine[objectname] Oueries value: Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[imagepath] Oueries value: HKLM\system\currentcontrolset\services\wbiosrvc[type] Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[start] Oueries value: HKLM\svstem\currentcontrolset\services\wbiosrvc[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\wbiosrvc[tag] HKLM\system\currentcontrolset\services\wbiosrvc[dependonservice] Oueries value: Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\wbiosrvc[group] Queries value: HKLM\system\currentcontrolset\services\wbiosrvc[objectname] Oueries value: HKLM\svstem\currentcontrolset\services\wcncsvc[imagepath] Oueries value: HKLM\system\currentcontrolset\services\wcncsvc[type] Oueries value: HKLM\system\currentcontrolset\services\wcncsvc[start] Oueries value: HKLM\system\currentcontrolset\services\wcncsvc[errorcontrol] Queries value: HKLM\system\currentcontrolset\services\wcncsvc[tag] HKLM\system\currentcontrolset\services\wcncsvc[dependonservice] Queries value: Queries value: HKLM\system\currentcontrolset\services\wcncsvc[dependongroup] Queries value: HKLM\system\currentcontrolset\services\wcncsvc[group] HKLM\system\currentcontrolset\services\wcncsvc[objectname] Queries value: Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[imagepath] Oueries value: HKLM\system\currentcontrolset\services\wcspluginservice[type] Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[start] Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[errorcontrol] Oueries value: HKLM\system\currentcontrolset\services\wcspluginservice[tag] Queries value: HKLM\system\currentcontrolset\services\wcspluginservice[dependongroup] Queries value: Oueries value: HKLM\system\currentcontrolset\services\wcspluginservice[group] HKLM\system\currentcontrolset\services\wcspluginservice[objectname] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\webclient[imagepath] Oueries value: HKLM\system\currentcontrolset\services\webclient[type] Queries value: HKLM\system\currentcontrolset\services\webclient[start] HKLM\system\currentcontrolset\services\webclient[errorcontrol] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\webclient[tag] Oueries value: HKLM\system\currentcontrolset\services\webclient[dependonservice] Oueries value: HKLM\system\currentcontrolset\services\webclient[dependongroup] Oueries value: HKLM\system\currentcontrolset\services\webclient[group] Queries value: HKLM\system\currentcontrolset\services\webclient[objectname] Oueries value: HKLM\system\currentcontrolset\services\wecsvc[imagepath] Queries value: HKLM\system\currentcontrolset\services\wecsvc[type]

```
Oueries value:
                        HKLM\system\currentcontrolset\services\wecsvc[start]
                        HKLM\system\currentcontrolset\services\wecsvc[errorcontrol]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\wecsvc[tag]
                        HKLM\system\currentcontrolset\services\wecsvc[dependonservice]
Queries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\wecsvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\wecsvc[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\wecsvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[start]
                        HKLM\system\currentcontrolset\services\wercplsupport[errorcontrol]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\wercplsupport[objectname]
Queries value:
                        HKLM\svstem\currentcontrolset\services\wersvc[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\wersvc[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\wersvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\wersvc[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\wersvc[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\wersvc[dependonservice]
Queries value:
                        HKLM\svstem\currentcontrolset\services\wersvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\wersvc[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\wersvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\winrm[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\winrm[type]
Queries value:
                        HKLM\system\currentcontrolset\services\winrm[start]
Queries value:
                        HKLM\system\currentcontrolset\services\winrm[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\winrm[tag]
Queries value:
                        HKLM\system\currentcontrolset\services\winrm[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\winrm[dependongroup]
                        HKLM\system\currentcontrolset\services\winrm[group]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\winrm[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\wlansvc[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\wlansvc[type]
Queries value:
                        HKLM\system\currentcontrolset\services\wlansvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\wlansvc[errorcontrol]
                        HKLM\system\currentcontrolset\services\wlansvc[tag]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\wlansvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\wlansvc[dependongroup]
                        HKLM\system\currentcontrolset\services\wlansvc[group]
Queries value:
Oueries value:
                        HKLM\svstem\currentcontrolset\services\wlansvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[imagepath]
                        HKLM\system\currentcontrolset\services\wmiapsrv[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[start]
Queries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[tag]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\wmiapsrv[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmiapsrv[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[start]
Queries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[errorcontrol]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[tag]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[dependongroup]
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[group]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\wpcsvc[imagepath]
                        HKLM\system\currentcontrolset\services\wpcsvc[type]
Queries value:
Queries value:
                        HKLM\system\currentcontrolset\services\wpcsvc[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\wpcsvc[errorcontrol]
                        HKLM\system\currentcontrolset\services\wpcsvc[tag]
Oueries value:
Queries value:
                        HKLM\system\currentcontrolset\services\wpcsvc[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\wpcsvc[dependongroup]
Queries value:
                        HKLM\system\currentcontrolset\services\wpcsvc[group]
                        HKLM\system\currentcontrolset\services\wpcsvc[objectname]
Oueries value:
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[imagepath]
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[type]
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[start]
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[errorcontrol]
Queries value:
                        HKLM\system\currentcontrolset\services\wsearch[tag]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\wsearch[dependonservice]
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[dependongroup]
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[group]
Oueries value:
                        HKLM\system\currentcontrolset\services\wsearch[objectname]
Oueries value:
                        HKLM\system\currentcontrolset\services\wuauserv[imagepath]
Queries value:
                        HKLM\system\currentcontrolset\services\wuauserv[type]
Oueries value:
                        HKLM\svstem\currentcontrolset\services\wuauserv[start]
Queries value:
                        HKLM\system\currentcontrolset\services\wuauserv[errorcontrol]
```

```
Oueries value:
                         HKLM\system\currentcontrolset\services\wuauserv[tag]
                         HKLM\system\currentcontrolset\services\wuauserv[dependonservice]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wuauserv[dependongroup]
 Queries value:
                         HKLM\system\currentcontrolset\services\wuauserv[group]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wuauserv[objectname]
 Queries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[start]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[errorcontrol]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[tag]
                         HKLM\system\currentcontrolset\services\wudfsvc[dependonservice]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[dependongroup]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[group]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc[objectname]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wwansvc[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wwansvc[type]
                         HKLM\system\currentcontrolset\services\wwansvc[start]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wwansvc[errorcontrol]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wwansvc[tag]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wwansvc[dependonservice]
 Queries value:
                         HKLM\system\currentcontrolset\services\wwansvc[dependongroup]
 Queries value:
                         HKLM\system\currentcontrolset\services\wwansvc[group]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wwansvc[objectname]
 Queries value:
                         HKLM\software\microsoft\windows
nt\currentversion\compatibility32[rundll32]
                         HKLM\software\microsoft\windows
 Queries value:
nt\currentversion\windows[loadappinit_dlls]
 Queries value:
                         HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
                         HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
 Queries value:
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
 Queries value:
                         HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
 Queries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
 Oueries value:
                         Queries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0ſdata21
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
 Queries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
 Queries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
                         HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\browser[imagepath]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[type]
                         HKLM\system\currentcontrolset\services\browser[start]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\browser[errorcontrol]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[tag]
 Oueries value:
                         HKLM\system\currentcontrolset\services\browser[dependonservice]
 Queries value:
                         HKLM\system\currentcontrolset\services\browser[dependongroup]
 Oueries 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]
 Oueries value:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
 Oueries value:
 Oueries value:
                         HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
```

HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]

HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]

HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]

HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]

Oueries value:

Queries value:

Oueries value:

Queries value:

```
Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
 Oueries value:
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
 Queries value:
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
 Queries value:
                          HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[imagepath]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[type]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[start]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\ikeext[tag]
 Queries value:
                          HKLM\system\currentcontrolset\services\ikeext[dependonservice]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ikeext[dependongroup]
 Oueries 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]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\ktmrm\triggerinfo\0[tvpe]
 Queries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
 Oueries value:
                          HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
 Oueries 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]
 Oueries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
 Oueries 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]
 Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]
 Oueries value:
HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]
                          HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
 Queries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
 Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
                         HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus policy agent \setminus trigger in fo \setminus 0 \ [data type 1]
                         Oueries value:
 Queries value:
                          HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
 Oueries value:
                          HKLM\svstem\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
 Queries value:
                         HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
 Oueries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
 Oueries value:
                          HKLM\system\currentcontrolset\services\storsyc\triggerinfo\0[type]
 Queries value:
                          HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
 Queries value:
                         HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
 Oueries value:
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
 Oueries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
 Queries value:
```

HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]

Queries value:

HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0] Queries value:

HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1] Queries value:

Queries value: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]

Queries value:

HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]

Oueries 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]

HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action] Oueries value: Oueries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type] Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid] Oueries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0] Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]

```
Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
 Oueries value:
                         HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
 Queries value:
 Oueries value:
                         HKLM\svstem\currentcontrolset\services\webclient\triggerinfo\0[type]
 Queries value:
                         HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
 Queries value:
                         HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
 Oueries value:
 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]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
 Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
 Oueries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
 Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
 Queries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
 Oueries value:
 Queries value:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
 Queries value:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
 Oueries value:
                         HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
 Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
 Oueries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
                         HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
 Oueries value:
                         HKCR\clsid\{660b90c8-73a9-4b58-8cae-
 Oueries value:
355b7f55341b}\inprocserver32[inprocserver32]
                         HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
 Queries value:
 Oueries value:
                         HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[threadingmodel]
                         HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
                         HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[threadingmodel]
                         HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
 Oueries value:
                         HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
 Queries value:
535773d48449}\inprocserver32[inprocserver32]
                         HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[threadingmodel]
 Queries value:
                         HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}[]
 Oueries value:
                         HKCR\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprocserver32[inprocserver32]
                         HKCR\clsid\{4c1fc63a-695c-47e8-a339-1a194be3d0b8}\inprocserver32[]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{4c1fc63a-695c-47e8-a339-
1a194be3d0b8}\inprocserver32[threadingmodel]
 Queries value:
                         HKLM\system\currentcontrolset\control\wmi\security[e0a40b26-30c4-4656-
bc9a-74a5c3a0b2ec]
 Queries value:
                         HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}[]
                         HKCR\clsid\{bfcd4a0c-06b6-4384-b768-
 Oueries value:
Odaa792c380e}\inprocserver32[inprocserver32]
                         HKCR\clsid\{bfcd4a0c-06b6-4384-b768-0daa792c380e}\inprocserver32[]
 Oueries value:
                         HKCR\clsid\{bfcd4a0c-06b6-4384-b768-
Odaa792c380e}\inprocserver32[threadingmodel]
 Queries value:
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}[]
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-
 Oueries value:
86d71067d145}\inprocserver32[inprocserver32]
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-86d71067d145}\inprocserver32[]
 Oueries value:
 Oueries value:
                         HKCR\clsid\{1d6322ad-aa85-4ef5-a828-
86d71067d145}\inprocserver32[threadingmodel]
 Sets/Creates value:
                         HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32[threadingmodel]
```

HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-

Sets/Creates value:

409d6c4515e9}\inprocserver32[]

Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]

Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\0000000000010[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000009[packedcatalogitem]

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[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\00000000005[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\0000000000002[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000009[packedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000
00000000006[packedcatalogitem]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\0000000000002[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem] Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[librarypath]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
Value changes:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath] Value changes:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace \ catalog 5 \ catalog \ entries 64 \ 000000000001 \ [library path]$

Value changes: HKLM\system\currentcontrolset\services\browser[start]
Value changes: HKLM\system\currentcontrolset\services\policyagent[start]