Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3331, Task ID: 834

Task ID:	834
Risk Level:	10
Date Processed:	2016-05-18 10:44:09 (UTC)
Processing Time:	80.5 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"
Sample ID:	3331
Type:	basic
Owner:	admin
Label:	1be5bc13fd1cf615a95feec0c5b7fd13
Date Added:	2016-05-18 10:30:52 (UTC)
File Type:	PE32:win32:gui
File Size:	201728 bytes
MD5:	1be5bc13fd1cf615a95feec0c5b7fd13
SHA256:	10e3f54492e5cdcdf2c1ae6d097aafdea9474ff77bf6ccb5a9c762ccb6e4a347
Description:	None

Pattern Matching Results

7 Writes to memory of system processes
6 Modifies registry autorun entries
6 Writes to system32 folder
5 Abnormal sleep detected
5 Installs service
10 Creates malicious events: ZeroAccess [Rootkit]
6 Changes Winsock providers
3 Connects to local host
4 Terminates process under Windows subfolder
4 Reads process memory
3 Long sleep detected
7 Injects thread into Windows process

Process/Thread Events

Creates process:	C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe ["C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"]
Creates process:	C:\Windows\SysWOW64\cmd.exe ["C:\Windows\system32\cmd.exe"]
Reads from process:	PID:2620 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:296 C:\Windows\explorer.exe
Writes to process:	PID:444 C:\Windows\System32\services.exe
Writes to process:	PID:2476 C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Terminates process:	C:\Windows\SysWOW64\cmd.exe
Creates remote thread:	C:\Windows\explorer.exe
Creates remote thread:	C:\Windows\System32\services.exe
Creates remote thread:	C:\Windows\System32\sppsvc.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\BaseNamedObjects\Restricted\{0C5AB9CD-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-0x00000000000009D8

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\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Creates:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Creates:	C:\$Recycle.Bin\S-1-5-18
Creates:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2
Creates:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\L
Creates:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Creates:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Creates:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Creates:	C:GAC_MSIL
Creates:	C:GAC

Creates:	C:GAC_32
Creates:	C:GAC_64
Creates:	C:\Windows\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
Creates:	C:\Windows\assembly\GAC_64\Desktop.ini
Creates:	C:\Windows\assembly\GAC_32\Desktop.ini
Opens:	C:\Windows\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-CFDFB467.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\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\includeincludeincludeincludeincludeinclude\
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\System32\Actioncenter.dll.3.Manifest
Opens:	C:\Windows\SysWOW64\WSHTCPIP.DLL
Opens:	C:\windows\temp\CRYPTSP.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Opens:	C:\Windows\MSWSOCK.dll
Opens:	C:\Windows\System32\mswsock.dll
Opens:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\n
Opens:	C:\Windows\assembly
Opens:	C:\Windows\assembly\GAC_32\Desktop.ini
Opens:	C:\Windows\assembly\GAC_64\Desktop.ini
Opens:	C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
Opens:	C:\Windows\System32\cryptsp.dll
Opens:	C:\Windows\System32\rsaenh.dll
Opens:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Opens:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\U
Opens:	C:\Windows\SysWOW64\cmd.exe
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb
Opens:	C:\
Opens:	C:\Windows\SysWOW64\ui\SwDRM.dll
Opens:	C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Opens:	C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
Opens:	C:\Windows\SysWOW64\winbrand.dll
Opens:	C:\Windows\SysWOW64\en-US\cmd.exe.mui
Opens:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Opens:	C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Opens:	C:\Windows\System32\en-US\setupapi.dll.mui
Opens:	C:\Windows\SysWOW64\calc.exe
Writes to:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Writes to:	C:\$Recycle.Bin\S-1-5-21-980053277-1733835069-2361817685-1001\$aaa1415b79b8dbbd8bd16c842c1858a2\n
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\System32\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
Writes to:	C:\Windows\assembly\GAC_64\Desktop.ini
Writes to:	C:\Windows\assembly\GAC_32\Desktop.ini
Reads from:	C:\Windows\SysWOW64\cmd.exe
Reads from:	C:\$Recycle.Bin\S-1-5-18\$aaa1415b79b8dbbd8bd16c842c1858a2\@
Reads from:	C:\Windows\System32\LogFiles\Scm\e22a8667-f75b-4ba9-ba46-067ed4429de8
Deletes:	C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe

Network Events

DNS query:	j.maxmind.com
DNS response:	j.maxmind.com ⇒ 127.0.0.1
Connects to:	127.0.0.1:80
Sends data to:	8.8.8.8:53
Sends data to:	83.133.123.20:53
Sends data to:	206.254.253.254:16470
Sends data to:	190.254.253.254:16470
Sends data to:	180.254.253.254:16470
Sends data to:	135.254.253.254:16470
Sends data to:	115.254.253.254:16470
Sends data to:	88.254.253.254:16470
Sends data to:	87.254.253.254:16470
Sends data to:	71.254.253.254:16470
Sends data to:	243.253.253.254:16470
Sends data to:	241.253.253.254:16470
Sends data to:	240.253.253.254:16470

Sends data to: 213.253.253.254:16470
Sends data to: 212.253.253.254:16470
Sends data to: 201.253.253.254:16470
Sends data to: 190.253.253.254:16470
Sends data to: 24.125.167.254:16470
Sends data to: 200.85.163.252:16470
Sends data to: 76.123.113.252:16470
Sends data to: 75.179.58.251:16470
Sends data to: 188.24.139.250:16470
Sends data to: 67.169.22.247:16470
Sends data to: 24.91.128.246:16470
Sends data to: 65.190.35.245:16470
Sends data to: 76.29.170.239:16470
Sends data to: 5.13.167.239:16470
Sends data to: 82.131.125.232:16470
Sends data to: 68.37.72.231:16470
Sends data to: 219.106.83.230:16470
Sends data to: 68.61.232.228:16470
Sends data to: 76.107.98.5:16470
Sends data to: 69.199.239.225:16470
Receives data from: 0.0.0.0:0

Windows Registry Events

Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100
Creates key: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101
Creates key: HKCU\software\microsoft\windows\currentversion\action center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
Creates key: HKCU\software\microsoft\windows\currentversion\action center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100
Creates key: HKCU\software\classes\clsid
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Creates key: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32
Deletes value: HKLM\software\microsoft\windows\currentversion\run[windows defender]
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution 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
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\language
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows 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
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters
Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\1e6c4482
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\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\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
Opens key: HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}
Opens key: HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Opens key: HKLM\software\microsoft\windows\currentversion\action center
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:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key: HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key: HKLM\software\policies\microsoft\cryptography
Opens key: HKLM\software\microsoft\cryptography
Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
Opens key:
HKLM\software\wow6432node\microsoft\cryptography\deshashsessionkeybackward
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{fd6905ce-952f-41f1-
9a6f-135d9c6622cc}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellserviceobjects\{f56f6fdd-aa9d-4618-
a949-c1b91af43b1a}
Opens key: HKLM\software\microsoft\windows\currentversion\run
Opens key: HKLM\software\wow6432node\microsoft\rpc
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key: HKLM\system\setup
Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\system\currentcontrolset\control\sqmservicelist

Opens key: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32
Opens key: HKLM\system\currentcontrolset\services\bfe
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\alg
Opens key: HKLM\system\currentcontrolset\services\alg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\appinfo
Opens key: HKLM\system\currentcontrolset\services\appinfo\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\appmgmt
Opens key: HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder
Opens key: HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\audiosrv
Opens key: HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\axinstsv
Opens key: HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
Opens key: HKLM\system\currentcontrolset\services\bdesvc
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
Opens key: HKLM\system\currentcontrolset\services\bfe\triggerinfo
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
Opens key: HKLM\system\currentcontrolset\services\bits
Opens key: HKLM\system\currentcontrolset\services\bits\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\0
Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\1
Opens key: HKLM\software\microsoft\cryptography\offload
Opens key: HKLM\software\microsoft\cryptography\deshashsessionkeybackward
Opens key: HKLM\system\currentcontrolset\services\browser\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper
Opens key: HKLM\system\currentcontrolset\services\rpcss
Opens key: HKLM\system\currentcontrolset\services\wuauserv
Opens key: HKLM\system\currentcontrolset\services\cryptsvc
Opens key: HKLM\system\currentcontrolset\services\bthserv
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\certpropsvc
Opens key: HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32
Opens key:

HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_32\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64
Opens key:
HKLM\system\currentcontrolset\services\clr_optimization_v2.0.50727_64\triggerinfo
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows\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\comsysapp
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
Opens key: HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\defragsvc
Opens key: HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\system\currentcontrolset\services\gpsvc
Opens key: HKLM\system\currentcontrolset\services\dhcp
Opens key: HKLM\system\currentcontrolset\services\dhcp\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\dot3svc
Opens key: HKLM\system\currentcontrolset\services\dot3svc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\dps
Opens key: HKLM\system\currentcontrolset\services\dps\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eaphost
Opens key: HKLM\system\currentcontrolset\services\eaphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\efs\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ehrecvr
Opens key: HKLM\system\currentcontrolset\services\ehrecvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ehsched
Opens key: HKLM\system\currentcontrolset\services\ehsched\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eventlog
Opens key: HKLM\system\currentcontrolset\services\eventlog\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\eventsystem
Opens key: HKLM\system\currentcontrolset\services\eventsystem\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fax
Opens key: HKLM\system\currentcontrolset\services\fax\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fdphost
Opens key: HKLM\system\currentcontrolset\services\fdphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fdrespub
Opens key: HKLM\system\currentcontrolset\services\fdrespub\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fontcache
Opens key: HKLM\system\currentcontrolset\services\fontcache\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0
Opens key: HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\hidserv
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\hkmsvc
Opens key: HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener
Opens key: HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider
Opens key: HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\idsvc
Opens key: HKLM\system\currentcontrolset\services\idsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ikeext
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\ipbusenum
Opens key: HKLM\system\currentcontrolset\services\ipbusenum\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ivmservice
Opens key: HKLM\system\currentcontrolset\services\keyiso
Opens key: HKLM\system\currentcontrolset\services\keyiso\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ktmrm
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lanmanserver
Opens key: HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation
Opens key: HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lltdsvc
Opens key: HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lmhosts
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\mcx2svc
Opens key: HKLM\system\currentcontrolset\services\mcx2svc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\mmcss
Opens key: HKLM\system\currentcontrolset\services\mmcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msdtc
Opens key: HKLM\system\currentcontrolset\services\msdtc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msiscsi
Opens key: HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\msiserver
Opens key: HKLM\system\currentcontrolset\services\msiserver\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\napagent
Opens key: HKLM\system\currentcontrolset\services\napagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netlogon
Opens key: HKLM\system\currentcontrolset\services\netlogon\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netman
Opens key: HKLM\system\currentcontrolset\services\netman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\netprofm
Opens key: HKLM\system\currentcontrolset\services\netprofm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing
Opens key: HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nlasvc
Opens key: HKLM\system\currentcontrolset\services\nlasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\nsi
Opens key: HKLM\system\currentcontrolset\services\nsi\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ose
Opens key: HKLM\system\currentcontrolset\services\ose\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc
Opens key: HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\p2psvc
Opens key: HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pcasvc
Opens key: HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc
Opens key: HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\perfhost
Opens key: HKLM\system\currentcontrolset\services\perfhost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pla
Opens key: HKLM\system\currentcontrolset\services\pla\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\plugplay
Opens key: HKLM\system\currentcontrolset\services\plugplay\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg
Opens key: HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc
Opens key: HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\power
Opens key: HKLM\system\currentcontrolset\services\power\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\profsvc
Opens key: HKLM\system\currentcontrolset\services\profsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\protectedstorage
Opens key: HKLM\system\currentcontrolset\services\protectedstorage\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\qwave
Opens key: HKLM\system\currentcontrolset\services\qwave\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rasauto
Opens key: HKLM\system\currentcontrolset\services\rasauto\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rasman
Opens key: HKLM\system\currentcontrolset\services\rasman\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteaccess
Opens key: HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\remoteregistry
Opens key: HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpclocator
Opens key: HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\rpcss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\samss
Opens key: HKLM\system\currentcontrolset\services\samss\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\scardsvr
Opens key: HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\schedule
Opens key: HKLM\system\currentcontrolset\services\schedule\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc
Opens key: HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sdrsvc
Opens key: HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\seclogon
Opens key: HKLM\system\currentcontrolset\services\seclogon\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sens
Opens key: HKLM\system\currentcontrolset\services\sens\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\sessionenv
Opens key: HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\shellhwdetection
Opens key: HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\snmptrap
Opens key: HKLM\system\currentcontrolset\services\snmptrap\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\spooler
Opens key: HKLM\system\currentcontrolset\services\spooler\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sppsvc
Opens key: HKLM\system\currentcontrolset\services\sppsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sppuinotify
Opens key: HKLM\system\currentcontrolset\services\sppuinotify\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv
Opens key: HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sstpsvc
Opens key: HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\stisvc
Opens key: HKLM\system\currentcontrolset\services\stisvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\swprv
Opens key: HKLM\system\currentcontrolset\services\swprv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\sysmain
Opens key: HKLM\system\currentcontrolset\services\sysmain\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\tapisrv
Opens key: HKLM\system\currentcontrolset\services\tapisrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tbs
Opens key: HKLM\system\currentcontrolset\services\tbs\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\termservice
Opens key: HKLM\system\currentcontrolset\services\termservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\themes
Opens key: HKLM\system\currentcontrolset\services\themes\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\threadorder
Opens key: HKLM\system\currentcontrolset\services\threadorder\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\tlntsvr
Opens key: HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\trkwks
Opens key: HKLM\system\currentcontrolset\services\trkwks\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\trustedinstaller
Opens key: HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\ui0detect
Opens key: HKLM\system\currentcontrolset\services\ui0detect\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\umrdpservice
Opens key: HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\upnphost
Opens key: HKLM\system\currentcontrolset\services\upnphost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\uxsms
Opens key: HKLM\system\currentcontrolset\services\uxsms\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vaultsvc
Opens key: HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vds
Opens key: HKLM\system\currentcontrolset\services\vds\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\vss
Opens key: HKLM\system\currentcontrolset\services\vss\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\w32time
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wbengine
Opens key: HKLM\system\currentcontrolset\services\wbengine\triggerinfo

Opens key: HKLM\system\currentcontrolset\services\wbiosrvc
Opens key: HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcncsvc
Opens key: HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice
Opens key: HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wdiservicehost
Opens key: HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost
Opens key: HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\webclient
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wecsvc
Opens key: HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wercplsupport
Opens key: HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc
Opens key: HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\winmgmt
Opens key: HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\winrm
Opens key: HKLM\system\currentcontrolset\services\winrm\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wlansvc
Opens key: HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wmiapsrv
Opens key: HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc
Opens key: HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpcsvc
Opens key: HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
Opens key: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
Opens key: HKLM\system\currentcontrolset\services\wscsvc
Opens key: HKLM\system\currentcontrolset\services\wscsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wsearch
Opens key: HKLM\system\currentcontrolset\services\wsearch\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wudfsvc
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
Opens key: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
Opens key: HKLM\system\currentcontrolset\services\wwansvc
Opens key: HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
Opens key: HKLM\system\currentcontrolset\services
Opens key: HKLM\system\currentcontrolset\services\wscsvc\parameters
Opens key: HKLM\system\currentcontrolset\services\wscsvc\security
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKCU\control panel\international
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key: HKLM\system\currentcontrolset\control\idconfigdb
Opens key: HKLM\system\currentcontrolset\control\idconfigdb\hardware profiles\0001
Opens key: HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\progid
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
Opens key: HKCR\wow6432node\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\devicenotificationcallbacks
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\deviceupdatelocations
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace

Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{35786d3c-
b075-49b9-88dd-029876e11c01}
Opens key: HKCU\software\classes\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder
Opens key: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserver32
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandler32
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32
Opens key: HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandler
Opens key: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\treatas
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{9113a02d-
00a3-46b9-bc5f-9c04daddd5d7}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{b155bdf8-
02f0-451e-9a26-ae317cfd7779}
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\mycomputer\namespace
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\mycomputer\namespace\delegatefolders
Opens key: HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder
Opens key: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder
Opens key: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\payloadoverride\skuid\55c92734-d682-4d71-983e-
d6ec3f16059f
Opens key: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\payloadoverride\appid\55c92734-d682-4d71-983e-
d6ec3f16059f
Opens key: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\referraldata\skuid\55c92734-d682-4d71-983e-
d6ec3f16059f
Opens key: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\referraldata\appid\55c92734-d682-4d71-983e-
d6ec3f16059f
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\progid
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}
Opens key: HKCR\wow6432node\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
Opens key: HKCU\software\classes\wow6432node\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\progid
Opens key: HKCR\wow6432node\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\progid
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserver32
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-
a00a-44d7-9371-beb064c98683}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{26ee0668-
a00a-44d7-9371-beb064c98683}\shellfolder
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandler32
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32
Opens key: HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandler
Opens key: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler
Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{35786d3c-
b075-49b9-88dd-029876e11c01}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{35786d3c-
b075-49b9-88dd-029876e11c01}\shellfolder
Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
Opens key: HKCU\software\classes\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\desktop\namespace\{21ec2020-3aea-1069-a2dd-08002b30309d}
Opens key: HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
Opens key: HKCU\software\classes\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder
Opens key: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder
Opens key: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{35786d3c-b075-49b9-88dd-029876e11c01}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{35786d3c-b075-49b9-88dd-029876e11c01}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder
Opens key: HKCU\software\classes\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder
Opens key: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\treatas
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}
Opens key: HKCU\software\classes\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key: HKCR\wow6432node\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\progid
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\treatas
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\treatas
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\progid
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
Opens key: HKCR\wow6432node\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
Opens key: HKCU\software\classes\wow6432node\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\progid
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler
Opens key: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}\inprochandler
Opens key: HKCR\wow6432node\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\progid
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler32
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler32
Opens key: HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler
Opens key: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprochandler

Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\treatas
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}
Opens key: HKCU\software\classes\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCR\wow6432node\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\progid
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler32
Opens key: HKCU\software\classes\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler
Opens key: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprochandler
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
Opens key: HKCU\software\classes\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCR\wow6432node\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\progid
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
Opens key: HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
Opens key: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\treatas
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\treatas
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\progid
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCR\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\progid
Opens key: HKCR\wow6432node\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\progid
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprochandler32
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprochandler32
Opens key: HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprochandler
Opens key: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprochandler
Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\controlpanel\namespace\namecustomizations
Opens key: HKLM\system\currentcontrolset\control\mui\stringcachesettings
Opens key: HKCU\software\classes\local settings\muicache\16\52c64b7e
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
Opens key: HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\hidedesktopicons\newstartpanel
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\hidedesktopicons\newstartpanel
Opens key: HKLM\software\microsoft\windows nt\currentversion\softwareprotectionplatform
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
Opens key: HKCU\software\classes\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCR\wow6432node\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\progid
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
Opens key: HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
Opens key: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\treatas
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\progid
Opens key: HKCU\software\classes\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}\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: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler32
Opens key: HKCU\software\classes\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler
Opens key: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprochandler
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\treatas
Opens key: HKCU\software\classes\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
Opens key: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCR\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}
Opens key: HKCU\software\classes\wow6432node\clsid\{90aa3a4e-1cba-4233-b8bb-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\{dd313e04-feff-11d1-8ecd-0000f87a470c}
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\treatas
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\treatas
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\progid
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid
Opens key: HKCU\software\classes\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}
Opens key: HKCR\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}
Opens key: HKCU\software\classes\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\progid
Opens key: HKCR\wow6432node\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\progid
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprocserver32
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprochandler32
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler32
Opens key: HKCU\software\classes\clsid\{dd313e04-feff-11d1-8ecd-
0000f87a470c}\inprochandler
Opens key: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprochandler
Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
Opens key: HKLM\software\microsoft\ctf\knownclasses
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disableusermodecallbackfilter]
Queries value: HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[1be5bc13fd1cf615a95feec0c5b7fd13]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]

Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
Queries value:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{dab69a6a-4d2a-4d44-94bf-e0091898c881}.check.100[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}[lastknownstate]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{11cd958a-c507-4ef3-b3f2-5fd9dfbd2c78}.check.101[checksetting]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{a5268b8e-7db5-465b-bab7-bdcda39a394a}[lastknownstate]
Queries value: HKCU\software\microsoft\windows\currentversion\action
center\checks\{a5268b8e-7db5-465b-bab7-bdcda39a394a}.check.100[checksetting]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
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\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[type]
Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[image path]
Queries value: HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
Queries value: HKLM\system\currentcontrolset\services\bfe[imagepath]
Queries value: HKLM\system\currentcontrolset\services\bfe[type]
Queries value: HKLM\system\currentcontrolset\services\bfe[start]
Queries value: HKLM\system\currentcontrolset\services\bfe[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\bfe[tag]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\bfe[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\bfe[group]
Queries value: HKLM\system\currentcontrolset\services\bfe[objectname]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]

Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
Queries value: HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
Queries value: HKLM\system\currentcontrolset\services\browser[imagepath]
Queries value: HKLM\system\currentcontrolset\services\browser[type]
Queries value: HKLM\system\currentcontrolset\services\browser[start]
Queries value: HKLM\system\currentcontrolset\services\browser[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\browser[tag]
Queries value: HKLM\system\currentcontrolset\services\browser[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\browser[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\browser[group]
Queries value: HKLM\system\currentcontrolset\services\browser[objectname]
Queries value: HKLM\system\currentcontrolset\services\dcomlaunch[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpceptmapper[objectname]
Queries value: HKLM\system\currentcontrolset\services\rpcss[objectname]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[objectname]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[imagepath]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[wow64]
Queries value: HKLM\system\currentcontrolset\services\wuauserv[requiredprivileges]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[type]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[start]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[group]
Queries value: HKLM\system\currentcontrolset\services\cryptsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[cmd]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[imagepath]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[type]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[start]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[tag]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[group]
Queries value: HKLM\system\currentcontrolset\services\gpsvc[objectname]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\dnscache[imagepath]
Queries value: HKLM\system\currentcontrolset\services\dnscache[type]
Queries value: HKLM\system\currentcontrolset\services\dnscache[start]
Queries value: HKLM\system\currentcontrolset\services\dnscache[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\dnscache[tag]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\dnscache[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\dnscache[group]
Queries value: HKLM\system\currentcontrolset\services\dnscache[objectname]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\ikeext[imagepath]

Queries value: HKLM\system\currentcontrolset\services\ikeext[type]
Queries value: HKLM\system\currentcontrolset\services\ikeext[start]
Queries value: HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\ikeext[tag]
Queries value: HKLM\system\currentcontrolset\services\ikeext[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\ikeext[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\ikeext[group]
Queries value: HKLM\system\currentcontrolset\services\ikeext[objectname]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
Queries value: HKLM\system\currentcontrolset\services\policyagent[imagepath]
Queries value: HKLM\system\currentcontrolset\services\policyagent[type]
Queries value: HKLM\system\currentcontrolset\services\policyagent[start]
Queries value: HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
Queries value: HKLM\system\currentcontrolset\services\policyagent[tag]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependonservice]
Queries value: HKLM\system\currentcontrolset\services\policyagent[dependongroup]
Queries value: HKLM\system\currentcontrolset\services\policyagent[group]
Queries value: HKLM\system\currentcontrolset\services\policyagent[objectname]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data1]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype2]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data2]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype3]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data3]
Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype4]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[guid]
Queries value: HKLM\system\currentcontrolset\services\w32time\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\webclient\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[action]

Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
Queries value: HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
Queries value: HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
Queries value: HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
Queries value: HKLM\system\currentcontrolset\control\idconfigdb[currentconfig]
Queries value:
HKLM\system\currentcontrolset\control\idconfigdb\currentdockinfo[dockingstate]
Queries value: HKLM\system\currentcontrolset\control\idconfigdb\hardware
profiles\0001[hwprofileguid]
Queries value: HKLM\system\currentcontrolset\control\idconfigdb\hardware
profiles\0001[friendlyname]
Queries value: HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders[suppressionpolicy]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders[]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{35786d3c-
b075-49b9-88dd-029876e11c01}[suppressionpolicy]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[attributes]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[wantsfordisplay]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{9113a02d-
00a3-46b9-bc5f-9c04daddd5d7}[suppressionpolicy]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{b155bdf8-
02f0-451e-9a26-ae317cfd7779}[suppressionpolicy]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[usedrophandler]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[wantsforparsing]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-
beb064c98683}\shellfolder[queryforoverlay]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\referraldata\appid\55c92734-d682-4d71-983e-
d6ec3f16059f[referralid]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[attributes]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-
029876e11c01}\shellfolder[wantsfordisplay]

Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[queryforinfotip]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hideinwebview]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hideondesktopperuser]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[usedrophandler]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[wantsforparsing]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[queryforoverlay]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[pintonamespacetree]
Queries value: HKCR\clsid\{26ee0668-a00a-44d7-9371-beb064c98683}\shellfolder[hasnavigationenum]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[queryforinfotip]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[hideinwebview]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[hideondesktopperuser]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[threadingmodel]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{26ee0668-a00a-44d7-9371-beb064c98683}]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[pintonamespacetree]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}\shellfolder[hasnavigationenum]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[sortorderindex]
Queries value: HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{35786d3c-b075-49b9-88dd-029876e11c01}]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[attributes]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}[sortorderindex]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[usedrophandler]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[wantsforparsing]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[queryforoverlay]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[queryforinfotip]

Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[hideinwebview]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[hideondesktopperuser]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[pintonamespacetree]
Queries value: HKCR\clsid\{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9113a02d-00a3-46b9-bc5f-9c04daddd5d7}]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[attributes]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[usedrophandler]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[wantsforparsing]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[queryforoverlay]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[queryforinfotip]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[hideinwebview]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[hideondesktopperuser]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[pintonamespacetree]
Queries value: HKCR\clsid\{b155bdf8-02f0-451e-9a26-ae317cfd7779}\shellfolder[hasnavigationenum]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{b155bdf8-02f0-451e-9a26-ae317cfd7779}]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[attributes]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[callforattributes]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[restrictedattributes]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[wantsfordisplay]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[hidefolderverbs]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[usedrophandler]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[wantsforparsing]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[wantsparsedisplayname]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[queryforoverlay]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[mapnetdriveverbs]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[queryforinfotip]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[hideinwebview]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder[hideondesktopperuser]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-

8d23b85255bf}\shellfolder[wantsaliasednotifications]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[wantsuniversaldelegate]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[nofilefolderjunction]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[pintonamespacetree]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[hasnavigationenum]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32[]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[loadwithoutcom]
Queries value: HKCR\clsid\{a47979d2-c419-11d9-a5b4-001185ad2b89}[]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}[]
Queries value: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-2299f0398e27}\inprocserver32[]
Queries value: HKCR\clsid\{1299cf18-c4f5-4b6a-bb0f-
2299f0398e27}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[]
Queries value: HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
Queries value: HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\inprocserver32[]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\inprocserver32[loadwithoutcom]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[sortorderindex]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}[system.itemnamedisplay]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[{b725f130-47ef-101a-
a5f1-02608c9eebac} 10]
Queries value: HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
Queries value:
HKLM\system\currentcontrolset\control\mui\stringcachesettings[stringcachegeneration]
Queries value: HKCU\software\classes\local
settings\muicache\16\52c64b7e[@c:\windows\system32\prnfldr.dll,-8036]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}[system.itemnamedisplay]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[{b725f130-47ef-101a-
a5f1-02608c9eebac} 10]
Queries value: HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
Queries value: HKCU\software\classes\local
settings\muicache\16\52c64b7e[@c:\windows\system32\netshell.dll,-1200]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.hideondesktop]
Queries value: HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2-
b5d6-00c04fd918d0} 34]
Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\hidedesktopicons\newstartpanel[{20d04fe0-
3aea-1069-a2d8-08002b30309d}]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[inactivityshutdowndelay]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[keeprunningthresholdmins]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32[]
Queries value: HKCR\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}[]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-a0b2badd77c8}\inprocserver32[]
Queries value: HKCR\clsid\{a2a9545d-a0c2-42b4-9708-
a0b2badd77c8}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}[]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-
535773d48449}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[]
Queries value: HKCR\clsid\{90aa3a4e-1cba-4233-b8bb-535773d48449}\inprocserver32[threadingmodel]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}[]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[inprocserver32]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[]
Queries value: HKCR\clsid\{dd313e04-feff-11d1-8ecd-0000f87a470c}\inprocserver32[threadingmodel]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[programs]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\user shell folders[common programs]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[favorites]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{9e3995ab-1f9c-4f13-b827-48b24b6c7174}]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[{52a4f021-7b75-48a9-9f6b-4b87a210bc8f}]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32[threadingmodel]
Sets/Creates value: HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}\inprocserver32[]
Sets/Creates value: HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[{q65231o0-o2s1-4857-n4pr-n8r7p6rn7q27}\pnyp.rkr]
Value changes: HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
Value changes: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[librarypath]
Value changes: HKLM\system\currentcontrolset\services\browser[start]
Value changes: HKLM\system\currentcontrolset\services\policyagent[start]
Value changes: HKCU\software\classes\local settings\muicache\16\52c64b7e[languagelist]

Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\userassist\{cebff5cd-ace2-4f4f-9178-9926f41749ea}\count[hrzr_pgyfrffvba]