Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	831
Risk Level:	10
Date Processed:	2016-05-18 10:43:53 (UTC)
Processing Time:	63.41 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

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

Process/Thread Events

Creates process:	C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe ["C:\windows\temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe"]
Creates process:	C:\Windows\system32\rundll32.exe [C:\Windows\system32\rundll32.exe bfe.dll,BfeOnServiceStartTypeChange]
Creates process:	C:\Windows\SysWOW64\cmd.exe ["C:\Windows\system32\cmd.exe"]
Creates process:	\SystemRoot\System32\Conhost.exe [\??\C:\Windows\system32\conhost.exe 0xffffffff]
Creates process:	C:\Windows\system32\taskhost.exe [taskhost.exe]
Creates process:	C:\Windows\system32\sppsvc.exe [C:\Windows\system32\sppsvc.exe]
Reads from process:	PID:1780 C:\Windows\SysWOW64\calc.exe
Writes to process:	PID:1120 C:\Windows\explorer.exe
Writes to process:	PID:480 C:\Windows\System32\services.exe
Writes to process:	PID:2148 C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
Terminates process:	C:\Windows\SysWOW64\cmd.exe
Terminates process:	C:\Windows\System32\conhost.exe
Terminates process:	C:\Windows\System32\rundll32.exe
Creates remote thread:	C:\Windows\explorer.exe
Creates remote thread:	C:\Windows\System32\services.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\DBWinMutex
Creates event:	\Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{0C5AB9CD-2F90-6754-8374-21D4DAB28CC1}
Creates event:	\Sessions\1\BaseNamedObjects\\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D78}
Creates event:	\BaseNamedObjects\\BaseNamedObjects\Restricted\{A3D35150-6823-4462-8C6E-7417FF841D77}
Creates event:	\Sessions\1\BaseNamedObjects\PRS_EXTERNAL_CHECK_CHANGED_NOTIFY
Creates event:	\Sessions\1\BaseNamedObjects\{43a2b8d7-6fed-4c18-bd36-b4630d61afb5}
Creates event:	\BaseNamedObjects\99b25af4-39cf-4c83-ad07-3c133e6d3135

File System Events

Creates:	C:\$Recycle.Bin\
Creates:	C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001
Creates:	C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3
Creates:	C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\L
Creates:	C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\U
Creates:	C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\@
Creates:	C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-1001\$915369118a4888a39e2f92dbd118adb3\n
Creates:	C:\$Recycle.Bin\S-1-5-18
Creates:	C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3
Creates:	C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\L
Creates:	C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\U
Creates:	C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
Creates:	C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
Creates:	C:GAC_MSIL
Creates:	C:\Windows\assembly\GAC
Creates:	C:GAC_32
Creates:	C:GAC_64
Creates:	C:\Windows\assembly\GAC_64\Desktop.ini
Creates:	C:\Windows\assembly\GAC_32\Desktop.ini
Creates:	C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
Creates:	C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
Creates:	C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
Creates:	C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC\statecache.lock
Creates:	C:\Windows\System32\spp\store\data.dat.tmp
Opens:	C:\Windows\Prefetch\1BE5BC13FD1CF615A95FEEC0C5B7F-CFDFB467.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll

```
  Opens:                  C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
  Opens:                  C:\Windows\SysWOW64\ntdll.dll
  Opens:                  C:\Windows\SysWOW64\kernel32.dll
  Opens:                  C:\Windows\SysWOW64\KernelBase.dll
  Opens:                  C:\Windows\apppatch\sysmain.sdb
  Opens:                  C:\Windows\SysWOW64\sechost.dll
  Opens:                  C:\Windows\SysWOW64\msvcrt.dll
  Opens:                  C:\Windows\SysWOW64\gdi32.dll
  Opens:                  C:\Windows\SysWOW64\user32.dll
  Opens:                  C:\Windows\SysWOW64\shlwapi.dll
  Opens:                  C:\Windows\SysWOW64\bcryptprimitives.dll
  Opens:                  C:\Windows\SysWOW64\cryptbase.dll
  Opens:                  C:\Windows\SysWOW64\sspicli.dll
  Opens:                  C:\Windows\SysWOW64\rpcrt4.dll
  Opens:                  C:\Windows\SysWOW64\advapi32.dll
  Opens:                  C:\Windows\SysWOW64\imm32.dll
  Opens:                  C:\Windows\SysWOW64\msctf.dll
  Opens:                  C:\Windows\SysWOW64\includeincludeincludeincludeincludeinclude\
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\SysWOW64\cabinet.dll
  Opens:                  C:\Windows\SysWOW64\nsi.dll
  Opens:                  C:\Windows\SysWOW64\ws2_32.dll
  Opens:                  C:\Windows\SysWOW64\mswsock.dll
  Opens:                  C:\Windows\SysWOW64\cryptsp.dll
  Opens:                  C:\Windows\SysWOW64\rsaenh.dll
  Opens:                  C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\n
  Opens:                  C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
  Opens:                  C:\Windows\assembly
  Opens:                  C:\Windows\assembly\GAC_32\Desktop.ini
  Opens:                  C:\Windows\assembly\GAC_64\Desktop.ini
  Opens:                  C:\Windows\System32\cryptsp.dll
  Opens:                  C:\Windows\System32\rsaenh.dll
  Opens:                  C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
  Opens:                  C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\U
  Opens:                  C:\Windows\System32\rundll32.exe
  Opens:                  C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
  Opens:                  C:\Windows\System32
  Opens:                  C:\Windows\System32\en-US\rundll32.exe.mui
  Opens:                  C:\Windows\System32\BFE.DLL
  Opens:                  C:\Windows\system32\bfe.dll.123.Manifest
  Opens:                  C:\Windows\system32\bfe.dll.124.Manifest
  Opens:                  C:\Windows\system32\bfe.dll.2.Manifest
  Opens:                  C:\Windows\System32\authz.dll
  Opens:                  C:\Windows\System32\dnsapi.dll
  Opens:                  C:\Windows\System32\sechost.dll
  Opens:                  C:\Windows\SysWOW64\cmd.exe
  Opens:                  C:\
  Opens:                  C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
  Opens:                  C:
  Opens:                  C:\Windows\Globalization
  Opens:                  C:\Windows\Globalization\Sorting
  Opens:                  C:\Windows\SysWOW64\wbem
  Opens:                  C:\Windows\System32\ntdll.dll
  Opens:                  C:\Windows\System32\wow64win.dll
  Opens:                  C:\Windows\System32\wow64cpu.dll
  Opens:                  C:\Windows\System32\kernel32.dll
  Opens:                  C:\Windows\System32\user32.dll
  Opens:                  C:\Windows\System32\locale.nls
  Opens:                  C:\Windows\SysWOW64\wbem\WMIC.exe
  Opens:                  C:\Windows\System32\conhost.exe
  Opens:                  C:\Windows\System32\combase.dll
  Opens:                  C:\Windows\System32\en-US\conhost.exe.mui
  Opens:                  C:\Windows\System32\ole32.dll
  Opens:                  C:\Windows\System32\uxtheme.dll
  Opens:                  C:\Windows\System32\cmd.exe
  Opens:                  C:\Windows\System32\en-US\cmd.exe.mui
  Opens:                  C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\@
  Opens:                  C:\Windows\System32\Tasks\Microsoft\Windows\WDI\ResolutionHost
  Opens:                  C:\Windows\System32\taskhost.exe
  Opens:                  C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
  Opens:                  C:\Windows\Prefetch\TASKHOST.EXE-CC5C42C1.pf
  Opens:                  C:\Windows\Performance
  Opens:                  C:\Windows\Performance\WinSAT
  Opens:                  C:\Windows\System32\en-US
  Opens:                  C:\Windows\System32\KernelBase.dll
  Opens:                  C:\Windows\System32\msvcrt.dll
  Opens:                  C:\Windows\System32\rpcrt4.dll
  Opens:                  C:\Windows\System32\oleaut32.dll
  Opens:                  C:\Windows\System32\rpcss.dll
  Opens:                  C:\Windows\System32\cryptbase.dll
  Opens:                  C:\Windows\System32\bcryptprimitives.dll
  Opens:                  C:\Windows\System32\gdi32.dll
  Opens:                  C:\Windows\System32\en-US\taskhost.exe.mui
  Opens:                  C:\Windows\System32\clbcatq.dll
  Opens:                  C:\Windows\System32\shlwapi.dll
  Opens:                  C:\Windows\System32\shell32.dll
  Opens:                  C:\Windows\System32\advapi32.dll
  Opens:                  C:\Windows\System32\SHCore.dll
  Opens:                  C:\Windows\System32\MemoryDiagnostic.dll
  Opens:                  C:\Windows\System32\fhsvcctl.dll
  Opens:                  C:\Windows\System32\regidle.dll
  Opens:                  C:\Windows\System32\pstask.dll
  Opens:                  C:\Windows\System32\imm32.dll
  Opens:                  C:\Windows\System32\dwmapi.dll
  Opens:                  C:\Windows\System32\wdi.dll
  Opens:                  C:\Windows\System32\radarrs.dll
  Opens:                  C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
  Opens:                  C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
  Opens:                  C:\Windows\System32\RstrtMgr.dll
  Opens:                  C:\Windows\System32\wer.dll
  Opens:                  C:\Windows\System32\version.dll
  Opens:                  C:\Windows\System32\ncrypt.dll
  Opens:                  C:\Windows\System32\bcrypt.dll
  Opens:                  C:\Windows\System32\ntasn1.dll
  Opens:                  C:\Windows\WindowsShell.Manifest
  Opens:                  C:\Windows\System32\en-US\radarrs.dll.mui
  Opens:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
  Opens:                    C:\Users\desktop.ini
  Opens:                    C:\Users
  Opens:                    C:\Users\Admin
  Opens:                    C:\Users\Admin\AppData
  Opens:                    C:\Users\Admin\AppData\Roaming
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\desktop.ini
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
  Opens:                    C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries
  Opens:                    C:\Users\Admin\Desktop\desktop.ini
  Opens:                    C:\Users\Public\desktop.ini
  Opens:                    C:\Users\Public
  Opens:                    C:\Users\Public\Desktop\desktop.ini
  Opens:                    C:\Windows\ServiceProfiles
  Opens:                    C:\Windows\System32\sppsvc.exe
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Adobe-Flash-For-Windows-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-ClientEdition-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Guest-Integration-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-Clients-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Management-PowerShell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Package-termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Hyper-V-Server-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Media-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Virtualization-Client-Interop-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Anytime-Upgrade-Results-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Mincore-
```

```
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-AvCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-ClientCore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Shell-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ApisetNamespace-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Backup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Basic-Http-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BLB-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-minkernel~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BootEnvironment-Dvd-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Branding-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-BusinessScanning-Feature-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
```

```
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-mincore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Features-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Client-Wired-Network-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CodecPack-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-COM-MSMQ-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-base~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-DriverClasses-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-vm~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-
vm~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Drivers-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Common-Modem-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CommonFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Com-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                   C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
```

```
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Net-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-RemoteFS-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Base-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Com-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-DS-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Mincore-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minio-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Minkernel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Net-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-CoreSystem-WOW64-Windows-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Dedup-ChunkLibrary-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-DirectoryServices-ADAM-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\microsoft-windows-directoryservices-adam-snapins-package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Disk-Diagnosis-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-Package~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Editions-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-FCI-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-
admin~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientExtensions-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
com~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
multimedia~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                 C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
termsrv~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
```

```
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-GroupPolicy-ClientTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-HandwritingRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Help-ClientUA-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ICM-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Identity-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IE-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-2-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-AddOn-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-IIS-WebServer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-Base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
Base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ImageBasedSetup-IE-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Optional-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-Package~31bf3856ad364e35~amd64~en-
US~10.0.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-InternetExplorer-
Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Killbits-Package~31bf3856ad364e35~amd64~~10.0.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Links-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Format-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Streaming-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Media-Streaming-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaCenter-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayback-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package-ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MediaPlayer-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Basic-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Premium-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-Sensors-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MobilePC-Client-SideShow-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-MSMQ-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
```

```
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
drivers~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Multilingual-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-
AutoNgenEnable.3.5~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-
NgenAssemblyExclusionClient~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Misc~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-MOF-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Perfcounters-
Extended~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-Typelibs~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
HttpNamespace~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
MsmqActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
PipeActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
TcpActivation~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WCF-
TcpPortSharing~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Shared-WPF-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-VCRedist-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx-Windows-Built-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx2-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package-
redist~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
```

```
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx3-WCF-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-US-OC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-NetFx4-WCF-US-OC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-OfflineFiles-UI-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ParentalControls-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerDist-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PeerToPeer-Full-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Personalization-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PhotoBasicPackage~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PlayToManager-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Portable-Devices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PowerShell-V2-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Presentation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printer-Drivers-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-Foundation-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-LocalPrinting-Home-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-PremiumTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Printing-XPSServices-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ProfessionalEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-ProfessionalWMCEdition~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-PsuedoTool-HashIDSpy-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasCMAK-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RasRip-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RDC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RecDisc-SDP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Redhawk-v1.0-package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-Client~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteAssistance-Package-
Client~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteDesktop-UserModeRDProtocol-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
LanguagePack~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RemoteFX-RemoteClient-Setup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-RotMgr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SearchEngine-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SecureStartup-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-APPXLOB-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-OCUR-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-Professional-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Security-SPP-Component-SKU-ProfessionalWMC-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ServicingBaseline-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-ShareMedia-ControlPanel-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-HomeGroup-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-SoundThemes-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Shell-Wallpaper-Common-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                    C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-SimpleTCP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-admin~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
admin~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-base~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
base~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-com~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-drivers~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ds~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
ds~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-enduser~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
enduser~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-inetsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
inetsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mergedcomponents~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mergedcomponents~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-mincore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
mincore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minio~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minio~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-minkernel~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
minkernel~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-multimedia~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
multimedia~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-net~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
net~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-printscan~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
printscan~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sdktools~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
sdktools~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-shell~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
shell~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-sql~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
sql~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
```

```
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-termsrv~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
termsrv~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-ua~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
ua~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-windows~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package-
windows~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SKU-Foundation-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SnippingTool-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SNMP-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SpeechRecognizer-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StickyNotes-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-StorageService-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Store-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Store-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-SystemRestore-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TabletPC-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Telnet-Server-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-CommandLineTools-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-MiscRedirection-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TerminalServices-WMIProvider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TextPrediction-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-TFTP-Client-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualPC-USB-RPM-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-VirtualXP-Licensing-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-Package~31bf3856ad364e35~amd64~en-
```

```
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WebcamExperience-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsFoundation-LanguagePack-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WindowsMediaPlayer-Troubleshooters-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinMDE-Package-avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinOcr-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WinSATMediaFiles-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMI-SNMP-Provider-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package-
avcore~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-WMPNetworkSharingService-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Microsoft-Windows-Xps-Foundation-Client-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Networking-MPSSVC-Rules-BusinessEdition-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\nt5.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\ntexe.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\ntpe.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\ntph.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\oem0.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Server-Help-Package.ClientProfessional~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-AM-Default-Definitions-
Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~en-
US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-Group-Policy-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~en-US~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\Windows-Defender-Package~31bf3856ad364e35~amd64~~6.2.9200.16384.cat
  Opens:                  C:\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-
00C04FC295EE}\windows-legacy-whql.cat
  Opens:                  C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
  Opens:                  C:\Windows\Branding
  Opens:                  C:\Windows\Branding\Basebrd
  Opens:                  C:\Windows\System32\en-US\sppsvc.exe.mui
  Opens:                  C:\Windows\System32\sppobjs.dll
  Opens:                  C:\Windows\Branding\Basebrd\basebrd.dll
  Opens:                  C:\Windows\System32\wwapi.dll
  Opens:                  C:\Windows\System32\wscinterop.dll
  Opens:                  C:\Windows\System32\wscapi.dll
  Opens:                  C:\Windows\System32\wscui.cpl
  Opens:                  C:\Windows\System32\wscinterop.dll.123.Manifest
  Opens:                  C:\Windows\System32\en-US\wscui.cpl.mui
  Opens:                  C:\Windows\System32\werconcpl.dll
  Opens:                  C:\Windows\System32\framedynos.dll
  Opens:                  C:\Windows\System32\wercplsupport.dll
  Opens:                  C:\Windows\System32\msxml6.dll
  Opens:                  C:\Windows\System32\msxml6r.dll
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ReportArchive
  Opens:                  C:\ProgramData\Microsoft\Windows\WER\ReportArchive
  Opens:                  C:\Users\Admin\AppData\Local\Microsoft\Windows\WER\ERC
  Opens:                  C:\Windows\System32\hcproviders.dll
  Opens:                  C:\Windows\System32\en-US\hcproviders.dll.mui
  Opens:                  C:\Program Files\Internet Explorer\ieproxy.dll
  Opens:                  C:\Windows\System32\en-US\ActionCenter.dll.mui
  Opens:                  C:\Windows\System32\Actioncenter.dll.3.Manifest
  Opens:                  C:\Windows\System32\spp\store\data.dat
  Opens:                  C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
  Opens:                  C:\Windows\System32\sppwinob.dll
  Opens:                  C:\Windows\System32\netapi32.dll
  Opens:                  C:\Windows\System32\netutils.dll
  Opens:                  C:\Windows\System32\srvcli.dll
  Opens:                  C:\Windows\System32\wkscli.dll
  Opens:                  C:\Windows\System32\dsrole.dll
  Opens:                  C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
manifest-signed.xrm-ms
  Opens:                  C:\Windows\System32\spp\store\cache\cache.dat
  Opens:                  C:\Windows\System32\spp\store\tokens.dat
  Opens:                  C:\Windows\System32\spp\store\data.dat.tmp
  Opens:                  C:\Windows\System32\spp\store
  Opens:                  C:\Windows\System32\spp\store\data.dat.bak
  Opens:                  C:\Windows\System32\en-US\KernelBase.dll.mui
  Opens:                  C:\Windows\System32\taskschd.dll
  Opens:                  C:\Windows\System32\sspicli.dll
  Writes to:              C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\@
  Writes to:              C:\$Recycle.Bin\S-1-5-21-1923240461-1905901954-2556564120-
1001\$915369118a4888a39e2f92dbd118adb3\n
  Writes to:              C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
  Writes to:              C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\n
  Writes to:              C:\Windows\assembly\GAC_64\Desktop.ini
  Writes to:              C:\Windows\assembly\GAC_32\Desktop.ini
  Writes to:              C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
  Writes to:              C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
  Writes to:              C:\Windows\System32\spp\store\data.dat.tmp
  Reads from:             C:\Windows\System32\LogFiles\Scm\115a30f5-9629-4e2e-993e-f2ef77734558
  Reads from:             C:\Windows\SysWOW64\cmd.exe
  Reads from:             C:\Windows\Prefetch\CMD.EXE-AC113AA8.pf
  Reads from:             C:\$Recycle.Bin\S-1-5-18\$915369118a4888a39e2f92dbd118adb3\@
  Reads from:             C:\Windows\System32\LogFiles\Scm\63268cc2-db2e-42f3-8133-2d5df404f513
  Reads from:             C:\Windows\Prefetch\TASKHOST.EXE-CC5C42C1.pf
  Reads from:
C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\CachedImage_1024_768_POS4.jpg
  Reads from:             C:\Users\desktop.ini
  Reads from:             C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
  Reads from:             C:\Users\Admin\Desktop\desktop.ini
  Reads from:             C:\Users\Public\desktop.ini
  Reads from:             C:\Users\Public\Desktop\desktop.ini
  Reads from:             C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
  Reads from:             C:\Windows\System32\spp\store\data.dat
  Reads from:             C:\Windows\System32\spp\plugin-manifests-signed\sppwinob-spp-plugin-
manifest-signed.xrm-ms
  Reads from:             C:\Windows\System32\spp\plugin-manifests-signed\sppobjs-spp-plugin-
manifest-signed.xrm-ms
  Reads from:             C:\Windows\System32\spp\store\cache\cache.dat
  Reads from:             C:\Windows\System32\spp\store\tokens.dat
  Deletes:                C:\Windows\Temp\1be5bc13fd1cf615a95feec0c5b7fd13.exe
  Deletes:                C:\Windows\System32\spp\store\data.dat.tmp
```

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
  Sends data to:          61.86.46.6:16470
  Sends data to:          94.112.235.6:16470
  Sends data to:          68.185.68.224:16470
  Sends data to:          74.12.46.223:16470
  Sends data to:          50.136.31.221:16470
  Sends data to:          173.21.26.221:16470
  Sends data to:          76.182.171.220:16470
  Sends data to:          118.8.112.220:16470
  Sends data to:          70.182.4.219:16470
  Sends data to:          98.85.39.13:16470
  Sends data to:          37.2.137.13:16470
  Sends data to:          184.89.197.216:16470
  Sends data to:          76.178.167.13:16470
  Sends data to:          200.30.249.214:16470
  Sends data to:          106.51.95.15:16470
  Sends data to:          174.7.120.16:16470
  Sends data to:          46.59.73.17:16470
  Sends data to:          31.41.65.21:16470
  Sends data to:          190.73.8.212:16470
  Sends data to:          180.196.236.210:16470
  Sends data to:          213.92.177.210:16470
  Sends data to:          174.48.147.210:16470
  Receives data from:         0.0.0.0:0
```

Windows Registry Events

```
  Creates key:                HKCU\software\classes\clsid
  Creates key:                HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-409d6c4515e9}
  Creates key:                HKCU\software\classes\clsid\{fbeb8a05-beee-4442-804e-
409d6c4515e9}\inprocserver32
  Creates key:                HKCU\software\microsoft\internet explorer\toolbar
  Creates key:                HKCU\software\microsoft\internet explorer\toolbar\shellbrowser
  Creates key:                HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\
  Creates key:                HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity
  Creates key:
HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14
  Creates key:                HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\
  Creates key:                HKLM\system\currentcontrolset\control\graphicsdrivers\configuration
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100
  Creates key:                HKCU\software\microsoft\windows\windows error reporting
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0
  Creates key:                HKCU\software\microsoft\windows\currentversion\startupnotify
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
  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\microsoft\windows\currentversion\action
center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}.check.800
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{134ea407-755d-4a93-b8a6-f290cd155023}.check.8001
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
  Creates key:                HKCU\software\microsoft\windows\currentversion\action
center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100
  Creates key:                HKLM\system\wpa
  Creates key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34
  Deletes value:              HKLM\software\microsoft\windows\currentversion\run[windows defender]
  Opens key:                  HKLM\software\microsoft\wow64
  Opens key:                  HKLM\system\currentcontrolset\control\terminal server
  Opens key:                  HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                  HKLM\system\currentcontrolset\control\srp\gp\dll
  Opens key:
HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                  HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:                  HKLM\system\currentcontrolset\control\nls\language
  Opens key:                  HKLM\system\currentcontrolset\control\mui\uilanguages
  Opens key:                  HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
  Opens key:                  HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
  Opens key:                  HKLM\software\wow6432node\policies\microsoft\mui\settings
  Opens key:                  HKLM\software\policies\microsoft\mui\settings
  Opens key:                  HKCU\
  Opens key:                  HKCU\control panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                  HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
  Opens key:                  HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                  HKCU\control panel\desktop\languageconfiguration
  Opens key:                  HKCU\control panel\desktop
  Opens key:                  HKCU\control panel\desktop\muicached
  Opens key:                  HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
  Opens key:                  HKLM\system\currentcontrolset\control\nls\sorting\versions
  Opens key:                  HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\gre_initialize
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
compatibility
  Opens key:                HKLM\
  Opens key:                HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  Opens key:                HKLM\system\currentcontrolset\control\nls\sorting\ids
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\system\currentcontrolset\control\compression
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog\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\00000014
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:
HKLM\software\policies\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
  Opens key:
HKLM\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
  Opens key:
HKCU\\software\microsoft\systemcertificates\root\certificates\2bd63d28d7bcd0e251195aeb519243c13142ebc3
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup migration\providers
  Opens key:                HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip
  Opens key:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\wow6432node\microsoft\cryptography\offload
  Opens key:
HKLM\software\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\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010
  Opens key:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKLM\software\microsoft\cryptography\deshashsessionkeybackward
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-18
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders
  Opens key:                HKU\.default\environment
  Opens key:                HKU\.default\volatile environment
  Opens key:                HKU\.default\volatile environment\0
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe\perfoptions
  Opens key:                HKU\.default\software\microsoft\windows
nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\rundll32.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\sidebyside
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options
  Opens key:                HKU\.default\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKU\.default\control
panel\desktop\muicached\machinelanguageconfiguration
  Opens key:                HKU\.default\software\policies\microsoft\control panel\desktop
  Opens key:                HKU\.default\control panel\desktop\languageconfiguration
  Opens key:                HKU\.default\control panel\desktop
  Opens key:                HKU\.default\control panel\desktop\muicached
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\system\currentcontrolset\services\bfe
  Opens key:                HKLM\system\currentcontrolset\services\bfe\startoverride
  Opens key:                HKLM\system\currentcontrolset\services\aelookupsvc
  Opens key:                HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\alg
  Opens key:                HKLM\system\currentcontrolset\services\alg\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\alluserinstallagent
  Opens key:                HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\appidsvc
  Opens key:                HKLM\system\currentcontrolset\services\appidsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\appinfo
  Opens key:                HKLM\system\currentcontrolset\services\appinfo\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\appmgmt
  Opens key:                HKLM\system\currentcontrolset\services\appmgmt\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\audioendpointbuilder
  Opens key:                HKLM\system\currentcontrolset\services\audioendpointbuilder\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\audiosrv
  Opens key:                HKLM\system\currentcontrolset\services\audiosrv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\axinstsv
  Opens key:                HKLM\system\currentcontrolset\services\axinstsv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\bfe\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bits
  Opens key:                HKLM\system\currentcontrolset\services\bits\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\brokerinfrastructure
  Opens key:                HKLM\system\currentcontrolset\services\brokerinfrastructure\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\browser
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\browser\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\browser\startoverride
  Opens key:                HKLM\system\currentcontrolset\services\bthserv
  Opens key:                HKLM\system\currentcontrolset\services\bthserv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\bthserv\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\certpropsvc
  Opens key:                HKLM\system\currentcontrolset\services\certpropsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\comsysapp
  Opens key:                HKLM\system\currentcontrolset\services\comsysapp\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\cryptsvc
  Opens key:                HKLM\system\currentcontrolset\services\cryptsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\cscservice
  Opens key:                HKLM\system\currentcontrolset\services\cscservice\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\cscservice\triggerinfo\1
  Opens key:                HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8
  Opens key:                HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows
  Opens key:                HKLM\software\microsoft\telemetryclient\throttlestore\sqm
  Opens key:                HKLM\software\microsoft\telemetryclient\throttlestore
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows
  Opens key:                HKLM\software\microsoft\telemetryclient\samplestore\sqm
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238528
  Opens key:
HKLM\software\microsoft\telemetryclient\throttlestore\sqm\windows\winsqm8\13238784
  Opens key:
HKLM\software\microsoft\telemetryclient\samplestore\sqm\windows\winsqm8\13238784
  Opens key:                HKLM\system\currentcontrolset\services\dcomlaunch
  Opens key:                HKLM\system\currentcontrolset\services\dcomlaunch\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\defragsvc
  Opens key:                HKLM\system\currentcontrolset\services\defragsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\deviceassociationservice
  Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo
  Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0
  Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1
  Opens key:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\deviceinstall
  Opens key:                HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\dhcp
  Opens key:                HKLM\system\currentcontrolset\services\dhcp\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dnscache
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\startoverride
  Opens key:                HKLM\system\currentcontrolset\services\dot3svc
  Opens key:                HKLM\system\currentcontrolset\services\dot3svc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dps
  Opens key:                HKLM\system\currentcontrolset\services\dps\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dsmsvc
  Opens key:                HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\eaphost
  Opens key:                HKLM\system\currentcontrolset\services\eaphost\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\efs
  Opens key:                HKLM\system\currentcontrolset\services\efs\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\efs\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\efs\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\eventlog
  Opens key:                HKLM\system\currentcontrolset\services\eventlog\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\eventsystem
  Opens key:                HKLM\system\currentcontrolset\services\eventsystem\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\fax
  Opens key:                HKLM\system\currentcontrolset\services\fax\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\fdphost
  Opens key:                HKLM\system\currentcontrolset\services\fdphost\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\fdrespub
  Opens key:                HKLM\system\currentcontrolset\services\fdrespub\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\fhsvc
  Opens key:                HKLM\system\currentcontrolset\services\fhsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\fontcache
  Opens key:                HKLM\system\currentcontrolset\services\fontcache\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\fontcache3.0.0.0
  Opens key:                HKLM\system\currentcontrolset\services\fontcache3.0.0.0\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\gpsvc
  Opens key:                HKLM\system\currentcontrolset\services\gpsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\hidserv
  Opens key:                HKLM\system\currentcontrolset\services\hidserv\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\hidserv\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\hkmsvc
  Opens key:                HKLM\system\currentcontrolset\services\hkmsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\homegrouplistener
  Opens key:                HKLM\system\currentcontrolset\services\homegrouplistener\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\homegroupprovider
  Opens key:                HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\ikeext
  Opens key:                HKLM\system\currentcontrolset\services\ikeext\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\ikeext\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\ikeext\startoverride
  Opens key:                HKLM\system\currentcontrolset\services\ivmservice
  Opens key:                HKLM\system\currentcontrolset\services\keyiso
  Opens key:                HKLM\system\currentcontrolset\services\keyiso\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\keyiso\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\ktmrm
  Opens key:                HKLM\system\currentcontrolset\services\ktmrm\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\lanmanserver
  Opens key:                HKLM\system\currentcontrolset\services\lanmanserver\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\lanmanworkstation
  Opens key:                HKLM\system\currentcontrolset\services\lanmanworkstation\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\lltdsvc
  Opens key:                HKLM\system\currentcontrolset\services\lltdsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\lmhosts
  Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\3
  Opens key:                HKLM\system\currentcontrolset\services\lsm
  Opens key:                HKLM\system\currentcontrolset\services\lsm\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\mmcss
  Opens key:                HKLM\system\currentcontrolset\services\mmcss\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\msdtc
  Opens key:                HKLM\system\currentcontrolset\services\msdtc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\msiscsi
  Opens key:                HKLM\system\currentcontrolset\services\msiscsi\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\msiserver
  Opens key:                HKLM\system\currentcontrolset\services\msiserver\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\napagent
  Opens key:                HKLM\system\currentcontrolset\services\napagent\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\ncasvc
  Opens key:                HKLM\system\currentcontrolset\services\ncasvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2
  Opens key:                HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\3
  Opens key:                HKLM\system\currentcontrolset\services\ncdautosetup
  Opens key:                HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\netlogon
  Opens key:                HKLM\system\currentcontrolset\services\netlogon\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\netman
  Opens key:                HKLM\system\currentcontrolset\services\netman\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\netprofm
  Opens key:                HKLM\system\currentcontrolset\services\netprofm\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\nettcpportsharing
  Opens key:                HKLM\system\currentcontrolset\services\nettcpportsharing\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\nlasvc
  Opens key:                HKLM\system\currentcontrolset\services\nlasvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\nsi
  Opens key:                HKLM\system\currentcontrolset\services\nsi\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\ose
  Opens key:                HKLM\system\currentcontrolset\services\ose\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\p2pimsvc
  Opens key:                HKLM\system\currentcontrolset\services\p2pimsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\p2psvc
  Opens key:                HKLM\system\currentcontrolset\services\p2psvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\pcasvc
  Opens key:                HKLM\system\currentcontrolset\services\pcasvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\peerdistsvc
  Opens key:                HKLM\system\currentcontrolset\services\peerdistsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\perfhost
  Opens key:                HKLM\system\currentcontrolset\services\perfhost\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\pla
  Opens key:                HKLM\system\currentcontrolset\services\pla\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\plugplay
  Opens key:                HKLM\system\currentcontrolset\services\plugplay\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\pnrpautoreg
  Opens key:                HKLM\system\currentcontrolset\services\pnrpautoreg\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\pnrpsvc
  Opens key:                HKLM\system\currentcontrolset\services\pnrpsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\policyagent
  Opens key:                HKLM\system\currentcontrolset\services\policyagent\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\policyagent\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\policyagent\startoverride
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cmd.exe
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\wow6432node\policies\microsoft\windows\appcompat
  Opens key:                HKLM\software\policies\microsoft\windows\appcompat
  Opens key:                HKCU\software\microsoft\windows nt\currentversion
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags
  Opens key:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
  Opens key:                HKLM\system\currentcontrolset\services\power
  Opens key:                HKLM\system\currentcontrolset\services\power\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\printnotify
  Opens key:                HKLM\system\currentcontrolset\services\printnotify\triggerinfo
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\cmd.exe
  Opens key:                HKLM\system\currentcontrolset\services\profsvc
  Opens key:                HKLM\system\currentcontrolset\services\profsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\qwave
  Opens key:                HKLM\system\currentcontrolset\services\qwave\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\rasauto
  Opens key:                HKLM\system\currentcontrolset\services\rasauto\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\rasman
  Opens key:                HKLM\system\currentcontrolset\services\rasman\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\remoteaccess
  Opens key:                HKLM\system\currentcontrolset\services\remoteaccess\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\remoteregistry
  Opens key:               HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\rpceptmapper
  Opens key:               HKLM\system\currentcontrolset\services\rpceptmapper\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\rpclocator
  Opens key:               HKLM\system\currentcontrolset\services\rpclocator\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\rpcss
  Opens key:               HKLM\system\currentcontrolset\services\rpcss\triggerinfo
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\conhost.exe
  Opens key:               HKLM\system\currentcontrolset\services\samss
  Opens key:               HKLM\system\currentcontrolset\services\samss\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\scardsvr
  Opens key:               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\2
  Opens key:               HKLM\system\currentcontrolset\services\schedule
  Opens key:               HKLM\system\currentcontrolset\services\schedule\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\scpolicysvc
  Opens key:               HKLM\system\currentcontrolset\services\scpolicysvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\sdrsvc
  Opens key:               HKLM\system\currentcontrolset\services\sdrsvc\triggerinfo
  Opens key:               HKLM\software\microsoft\ole
  Opens key:               HKLM\software\microsoft\ole\tracing
  Opens key:               HKLM\software\microsoft\oleaut
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\console\truetypefont
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\console\fullscreen
  Opens key:               HKLM\system\currentcontrolset\services\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:               HKCU\console
  Opens key:               HKCU\console\
  Opens key:               HKLM\system\currentcontrolset\services\sensrsvc
  Opens key:               HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2
  Opens key:               HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\3
  Opens key:               HKLM\system\currentcontrolset\services\sessionenv
  Opens key:               HKLM\system\currentcontrolset\services\sessionenv\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\shellhwdetection
  Opens key:               HKLM\system\currentcontrolset\services\shellhwdetection\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\snmptrap
  Opens key:               HKLM\system\currentcontrolset\services\snmptrap\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\spooler
  Opens key:               HKLM\system\currentcontrolset\services\spooler\triggerinfo
  Opens key:               HKCU\console\%systemroot%_system32_cmd.exe
  Opens key:               HKCU\console\%systemroot%\system32\cmd.exe
  Opens key:               HKLM\system\currentcontrolset\services\sppsvc
  Opens key:               HKLM\system\currentcontrolset\services\sppsvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\control\nls\locale
  Opens key:               HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
  Opens key:               HKLM\system\currentcontrolset\control\nls\language groups
  Opens key:               HKLM\system\currentcontrolset\services\ssdpsrv
  Opens key:               HKLM\system\currentcontrolset\services\ssdpsrv\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange
  Opens key:               HKLM\system\currentcontrolset\services\sstpsvc
  Opens key:               HKLM\system\currentcontrolset\services\sstpsvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\stisvc
  Opens key:               HKLM\system\currentcontrolset\services\stisvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\storsvc
  Opens key:               HKLM\system\currentcontrolset\services\storsvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\storsvc\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\svsvc
  Opens key:               HKLM\system\currentcontrolset\services\svsvc\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\svsvc\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\swprv
  Opens key:               HKLM\system\currentcontrolset\services\swprv\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\sysmain
  Opens key:               HKLM\system\currentcontrolset\services\sysmain\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\systemeventsbroker
  Opens key:               HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\2
  Opens key:               HKLM\system\currentcontrolset\services\tabletinputservice
  Opens key:               HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\tapisrv
  Opens key:               HKLM\system\currentcontrolset\services\tapisrv\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\termservice
  Opens key:               HKLM\system\currentcontrolset\services\termservice\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\themes
  Opens key:               HKLM\system\currentcontrolset\services\themes\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\threadorder
  Opens key:               HKLM\system\currentcontrolset\services\threadorder\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\timebroker
  Opens key:               HKLM\system\currentcontrolset\services\timebroker\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\timebroker\triggerinfo\0
  Opens key:               HKLM\system\currentcontrolset\services\timebroker\triggerinfo\1
  Opens key:               HKLM\system\currentcontrolset\services\timebroker\triggerinfo\2
  Opens key:               HKLM\system\currentcontrolset\services\tlntsvr
  Opens key:               HKLM\system\currentcontrolset\services\tlntsvr\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\trkwks
  Opens key:               HKLM\system\currentcontrolset\services\trkwks\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\trustedinstaller
  Opens key:               HKLM\system\currentcontrolset\services\trustedinstaller\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\ui0detect
  Opens key:               HKLM\system\currentcontrolset\services\ui0detect\triggerinfo
  Opens key:               HKLM\system\currentcontrolset\services\umrdpservice
  Opens key:               HKLM\system\currentcontrolset\services\umrdpservice\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\upnphost
Opens key:                HKLM\system\currentcontrolset\services\upnphost\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vaultsvc
Opens key:                HKLM\system\currentcontrolset\services\vaultsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vds
Opens key:                HKLM\system\currentcontrolset\services\vds\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmicheartbeat
Opens key:                HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\vmicheartbeat\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\vmickvpexchange
Opens key:                HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\vmickvpexchange\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\vmicrdv
Opens key:                HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\vmicrdv\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\vmicshutdown
Opens key:                HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\vmicshutdown\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\vmictimesync
Opens key:                HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\vmictimesync\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\vmicvss
Opens key:                HKLM\system\currentcontrolset\services\vmicvss\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\vmicvss\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\vss
Opens key:                HKLM\system\currentcontrolset\services\vss\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\w32time
Opens key:                HKLM\system\currentcontrolset\services\w32time\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\w32time\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\w32time\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\w32time\triggerinfo\2
Opens key:                HKLM\system\currentcontrolset\services\wbengine
Opens key:                HKLM\system\currentcontrolset\services\wbengine\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wbiosrvc
Opens key:                HKLM\system\currentcontrolset\services\wbiosrvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wcmsvc
Opens key:                HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\wcmsvc\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wcncsvc
Opens key:                HKLM\system\currentcontrolset\services\wcncsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wcspluginservice
Opens key:                HKLM\system\currentcontrolset\services\wcspluginservice\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wdiservicehost
Opens key:                HKLM\system\currentcontrolset\services\wdiservicehost\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wdisystemhost
Opens key:                HKLM\system\currentcontrolset\services\wdisystemhost\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\webclient
Opens key:                HKLM\system\currentcontrolset\services\webclient\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\webclient\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\webclient\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wecsvc
Opens key:                HKLM\system\currentcontrolset\services\wecsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wercplsupport
Opens key:                HKLM\system\currentcontrolset\services\wercplsupport\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wersvc
Opens key:                HKLM\system\currentcontrolset\services\wersvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wersvc\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\wersvc\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wiarpc
Opens key:                HKLM\system\currentcontrolset\services\wiarpc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\windefend
Opens key:                HKLM\system\currentcontrolset\services\windefend\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\windefend\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\windefend\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\winhttpautoproxysvc
Opens key:                HKLM\system\currentcontrolset\services\winhttpautoproxysvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\winmgmt
Opens key:                HKLM\system\currentcontrolset\services\winmgmt\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\winrm
Opens key:                HKLM\system\currentcontrolset\services\winrm\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wlansvc
Opens key:                HKLM\system\currentcontrolset\services\wlansvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wlidsvc
Opens key:                HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wlidsvc\triggerinfo\2
Opens key:                HKLM\system\currentcontrolset\services\wmiapsrv
Opens key:                HKLM\system\currentcontrolset\services\wmiapsrv\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wmpnetworksvc
Opens key:                HKLM\system\currentcontrolset\services\wmpnetworksvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wpcsvc
Opens key:                HKLM\system\currentcontrolset\services\wpcsvc\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4
Opens key:                HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\5
Opens key:                HKLM\system\currentcontrolset\services\wsearch
Opens key:                HKLM\system\currentcontrolset\services\wsearch\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wsservice
Opens key:                HKLM\system\currentcontrolset\services\wsservice\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\wsservice\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wuauserv
Opens key:                HKLM\system\currentcontrolset\services\wuauserv\triggerinfo
Opens key:                HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0
Opens key:                HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1
Opens key:                HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\2
Opens key:                HKLM\system\currentcontrolset\services\wudfsvc
```

```
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0
  Opens key:                HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\1
  Opens key:                HKLM\system\currentcontrolset\services\wwansvc
  Opens key:                HKLM\system\currentcontrolset\services\wwansvc\triggerinfo
  Opens key:                HKU\s-1-5-21-1923240461-1905901954-2556564120-1001
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001
  Opens key:                HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows\currentversion\explorer\user shell folders
  Opens key:                HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\environment
  Opens key:                HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\volatile environment
  Opens key:                HKU\s-1-5-21-1923240461-1905901954-2556564120-1001\volatile
environment\0
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\taskhost.exe
  Opens key:                HKLM\system\currentcontrolset\control\session manager\quota system\s-1-
5-21-1923240461-1905901954-2556564120-1001
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\taskhost.exe
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\appid\taskhost.exe
  Opens key:                HKCR\appid\taskhost.exe
  Opens key:                HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}
  Opens key:                HKCR\activatableclasses\clsid
  Opens key:                HKCR\activatableclasses\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
  Opens key:                HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
  Opens key:                HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}
  Opens key:                HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\treatas
  Opens key:                HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\treatas
  Opens key:                HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\inprocserver32
  Opens key:                HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\inprochandler32
  Opens key:                HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\inprochandler
  Opens key:                HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprochandler
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
a37a-4f91-bdba-fbb98fe804bf}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8-e3670ed91517}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
393e-41c3-9885-29ec5a701926}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
10bc-4f96-9b21-4b6b83dbf476}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
fd02-4b82-a0a5-783266e430ab}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
5780-49de-9eb5-8d53a51fd146}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
398d-4edb-af71-3b830219abf7}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{63e0d0f7-
ac2f-493b-a7f2-2f3ccdb66fca}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
6c5b-43bb-860b-d47ae85242b1}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b-d429828bea2e}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{7a54f16f-
a73a-4258-ba46-a1e998a6aa74}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9-
809a-482b-b60b-bcad1f8d0cd7}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8cc29128-
0b57-4a2b-a7b9-a74a70ba6fa1}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6a50bbff5d15}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da-
b965-4fc3-8781-88dd50a6299d}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
3f06-411b-9dd5-35bc5666ff3e}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
a6ca-48e0-a7c4-4cdd258439e2}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
a840-44a9-97b1-fb74fddaa8c8}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
60e9-4301-a338-beab1c70b3e9}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a068e}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c0f51d84-
11b9-4e74-b083-99f11ba2db0a}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c8544339-
5be9-4f25-862e-485f1b1a6935}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-
3852-4952-b76b-23bb8e35d344}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
3287-4e3f-af68-632c90f3ac95}
  Opens key:                HKLM\system\currentcontrolset\control\wdi\config
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
```

```
   Opens key:                 HKLM\system\currentcontrolset\control
   Opens key:                 HKLM\software\microsoft\restartmanager
   Opens key:                 HKLM\software\microsoft\windows\windows error reporting\wmr
   Opens key:                 HKCU\software\microsoft\windows\currentversion\radar
   Opens key:                 HKLM\software\microsoft\radar\heapleakdetection\settings
   Opens key:                 HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}
   Opens key:                 HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}
   Opens key:                 HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\treatas
   Opens key:                 HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\treatas
   Opens key:                 HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\inprocserver32
   Opens key:                 HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\inprochandler32
   Opens key:                 HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\inprochandler
   Opens key:                 HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprochandler
   Opens key:                 HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
   Opens key:                 HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
   Opens key:                 HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\treatas
   Opens key:                 HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\treatas
   Opens key:                 HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprocserver32
   Opens key:                 HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprochandler32
   Opens key:                 HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprochandler
   Opens key:                 HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprochandler
   Opens key:                 HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
   Opens key:                 HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}
   Opens key:                 HKCU\software\classes\interface\{dbea162d-04e8-460f-8a0b-
4a431715d9a3}\proxystubclsid32
   Opens key:                 HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32
   Opens key:                 HKLM\software\policies\microsoft\windows\edgeui
   Opens key:                 HKCU\software\policies\microsoft\windows\edgeui
   Opens key:                 HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
   Opens key:                 HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}
   Opens key:                 HKCU\software\classes\interface\{92ca9dcd-5622-4bba-a805-
5e9f541bd8c9}\proxystubclsid32
   Opens key:                 HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32
   Opens key:                 HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}
   Opens key:                 HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}
   Opens key:                 HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\treatas
   Opens key:                 HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\treatas
   Opens key:                 HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32
   Opens key:                 HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprochandler32
   Opens key:                 HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprochandler
   Opens key:                 HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprochandler
   Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\advanced
   Opens key:                 HKLM\system\currentcontrolset\enum\swd\printenum\printqueues
   Opens key:                 HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties
   Opens key:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{afd97640-86a3-4210-b67c-
289c41aabe55}\0002
   Opens key:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{afd97640-86a3-4210-b67c-
289c41aabe55}\0003
   Opens key:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{a45c254e-df1c-4efd-8020-
67d146a850e0}\0011
   Opens key:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues\properties\{8c7ed206-3f8a-4827-b3ab-
ae9e1faefc6c}\0002
   Opens key:                 HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
   Opens key:                 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}
   Opens key:                 HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\treatas
   Opens key:                 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\treatas
   Opens key:                 HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprocserver32
   Opens key:                 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler32
   Opens key:                 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{660b90c8-73a9-4b58-8cae-
355b7f55341b}\inprochandler
   Opens key:                 HKCR\clsid\{660b90c8-73a9-4b58-8cae-355b7f55341b}\inprochandler
   Opens key:                 HKCU\software\classes\applications\calc.exe
   Opens key:                 HKCR\applications\calc.exe
   Opens key:                 HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
   Opens key:                 HKLM\software\policies\microsoft\windows\control panel\desktop
   Opens key:                 HKCU\software\policies\microsoft\windows\control panel\desktop
   Opens key:                 HKCU\software\microsoft\internet explorer\toolbar
   Opens key:                 HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}
   Opens key:                 HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}
   Opens key:                 HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\treatas
   Opens key:                 HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\treatas
   Opens key:                 HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprocserver32
   Opens key:                 HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprocserver32
   Opens key:                 HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprochandler32
   Opens key:                 HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprochandler
   Opens key:                 HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprochandler
   Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\commandstore
```

```
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\commandstore\
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar\
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{031e4825-7b94-4dc3-
b131-e946b44c8dd5}
  Opens key:                HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}
  Opens key:                HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}
  Opens key:                HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\treatas
  Opens key:                HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\treatas
  Opens key:                HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprocserver32
  Opens key:                HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprochandler32
  Opens key:                HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprochandler
  Opens key:                HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
  Opens key:                HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}
  Opens key:                HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\treatas
  Opens key:                HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\treatas
  Opens key:                HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32
  Opens key:                HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler32
  Opens key:                HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprochandler
  Opens key:                HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
  Opens key:                HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}
  Opens key:                HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
  Opens key:                HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}
  Opens key:                HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\treatas
  Opens key:                HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\treatas
  Opens key:                HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprocserver32
  Opens key:                HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprochandler32
  Opens key:                HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprochandler
  Opens key:                HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprochandler
  Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffff_ffffffff_0^cc77560bc3634a486857716562968286
  Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14
  Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_ryi0001 agnieszka
01_1d_07d7_b2_1414_008d_ffffffff_ffffffff_0^700ef59a5da31cbd79f31237af2ad4c4
  Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0_00_07db_c6^182fdc0875f0a76803e4a9848a8c1ea7
  Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00
  Opens key:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003
  Opens key:                HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
11e3-be67-0800272f6e60}
  Opens key:                HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
11e3-be67-0800272f6e60}\properties
  Opens key:                HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0002
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{3b2ce006-5e61-4fde-bab8-9b8aac9b26df}\0001
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0002
  Opens key:                HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
11e3-be67-0800272f6e60}
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{afd97640-86a3-4210-b67c-289c41aabe55}\0003
  Opens key:                HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
11e3-be67-0800272f6e60}\properties
  Opens key:                HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{a45c254e-df1c-4efd-8020-67d146a850e0}\0011
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{8c7ed206-3f8a-4827-b3ab-ae9e1faefc6c}\0002
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{3b2ce006-5e61-4fde-bab8-9b8aac9b26df}\0001
  Opens key:                HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
```

```
b32c-cd2da77617c7}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\devicenotificationcallbacks
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\deviceupdatelocations
   Opens key:                 HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
   Opens key:                 HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}
   Opens key:                 HKCU\software\classes\clsid\{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\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder
   Opens key:                 HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}\shellfolder
   Opens key:                 HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\treatas
   Opens key:                 HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\treatas
   Opens key:                 HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32
   Opens key:                 HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32
   Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{21ec2020-
3aea-1069-a2dd-08002b30309d}\shellfolder
   Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{21ec2020-
3aea-1069-a2dd-08002b30309d}\shellfolder
   Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\nonenum
   Opens key:                 HKLM\software\microsoft\windows\currentversion\policies\nonenum
   Opens key:                 HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler32
   Opens key:                 HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprochandler
   Opens key:                 HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprochandler
   Opens key:                 HKCU\software\classes\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}
   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\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}
   Opens key:                 HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}
   Opens key:                 HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\treatas
   Opens key:                 HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\treatas
   Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{35786d3c-b075-
49b9-88dd-029876e11c01}
   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\{289af617-
1cc3-42a6-926c-e6a863f0e3ba}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{35786d3c-
b075-49b9-88dd-029876e11c01}
   Opens key:                 HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprocserver32
   Opens key:                 HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32
   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\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
   Opens key:                 HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprochandler32
   Opens key:                 HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler32
   Opens key:                 HKCU\software\classes\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprochandler
   Opens key:                 HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprochandler
   Opens key:                 HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
   Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\controlpanel\namespace\{9c73f5e5-7ae7-
4e32-a8e8-8d23b85255bf}
   Opens key:                 HKCU\software\classes\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder
   Opens key:                 HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\shellfolder
   Opens key:
HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations
   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:                 HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}\inprocserver32
   Opens key:                 HKLM\software\microsoft\windows\currentversion\shell extensions\blocked
   Opens key:                 HKCU\software\microsoft\windows\currentversion\shell extensions\blocked
   Opens key:                 HKCU\software\microsoft\windows\currentversion\shell extensions\cached
   Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}
   Opens key:                 HKCR\activatableclasses\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}
   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}\inprocserver32
   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:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}\
  Opens key:                HKCU\software\classes\drive\shellex\folderextensions
  Opens key:                HKCR\drive\shellex\folderextensions
  Opens key:                HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
  Opens key:                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{9c73f5e5-7ae7-4e32-
a8e8-8d23b85255bf}
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userslibraries\namespace
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders\{896664f7-
12e1-490f-8782-c0835afd98fc}
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\userslibraries\namespace
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\userslibraries\namespace\delegatefolders
  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:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\shellex\iconhandler
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\defaulticon
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\desktop\namespace\namecustomizations
  Opens key:                HKLM\system\currentcontrolset\services\bits\startoverride
  Opens key:                HKLM\system\currentcontrolset\services\http
  Opens key:                HKU\s-1-5-20
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-20
  Opens key:                HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders
  Opens key:                HKU\s-1-5-20\environment
  Opens key:                HKU\s-1-5-20\volatile environment
  Opens key:                HKU\s-1-5-20\volatile environment\0
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sppsvc.exe
  Opens key:                HKLM\system\currentcontrolset\control\session manager\quota system\s-1-
5-20
  Opens key:                HKLM\system\currentcontrolset\control\mui\settings
  Opens key:                HKLM\software\classes
  Opens key:                HKCR\appid\sppsvc.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}
  Opens key:                HKCR\activatableclasses\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:                HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:                HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}
  Opens key:                HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\treatas
  Opens key:                HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\treatas
  Opens key:                HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32
  Opens key:                HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprochandler32
  Opens key:                HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprochandler
  Opens key:                HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprochandler
  Opens key:                HKLM\software\microsoft\security center
  Opens key:                HKLM\software\policies\microsoft\internet explorer\security
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\4
  Opens key:                HKCU\software\policies\microsoft\internet explorer
  Opens key:                HKCU\software\microsoft\internet explorer\security
  Opens key:                HKLM\software\microsoft\internet explorer\security
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings\zones
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{ca236752-2e77-4386-b63b-0e34774a413d}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}
  Opens key:                HKCR\activatableclasses\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
  Opens key:                HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
  Opens key:                HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}
  Opens key:                HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\treatas
  Opens key:                HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\treatas
  Opens key:                HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32
  Opens key:                HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler32
  Opens key:                HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprochandler
  Opens key:                HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprochandler
  Opens key:                HKLM\software\microsoft\wbem\cimom
  Opens key:                HKLM\software\policies\microsoft\windows\windows error reporting
  Opens key:                HKLM\software\microsoft\windows\windows error reporting
  Opens key:                HKCU\software\policies\microsoft\windows\windows error reporting
  Opens key:                HKCU\software\microsoft\windows\windows error reporting
  Opens key:                HKLM\software\microsoft\windows\windows error reporting\syspreplock
  Opens key:                HKCU\software\microsoft\windows\windows error reporting\erc
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}
  Opens key:                HKCR\activatableclasses\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
  Opens key:                HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
  Opens key:                HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}
  Opens key:                HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\treatas
  Opens key:                HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\treatas
  Opens key:                HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32
  Opens key:                HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprochandler32
  Opens key:                HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprochandler
  Opens key:                HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:                HKLM\software\microsoft\msxml60
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{c8e6f269-b90a-4053-a3be-499afcec98c4}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}
  Opens key:                HKCR\activatableclasses\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
  Opens key:                HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
  Opens key:                HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}
  Opens key:                HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\treatas
  Opens key:                HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\treatas
  Opens key:                HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32
  Opens key:                HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprochandler32
  Opens key:                HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprochandler
  Opens key:                HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprochandler
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\system
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}
  Opens key:                HKCR\activatableclasses\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
  Opens key:                HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
  Opens key:                HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}
  Opens key:                HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\treatas
  Opens key:                HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\treatas
  Opens key:                HKCR\activatableclasses\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
  Opens key:                HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
  Opens key:                HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}
  Opens key:                HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\treatas
  Opens key:                HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\treatas
  Opens key:                HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32
  Opens key:                HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32
  Opens key:                HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprochandler32
  Opens key:                HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprochandler
  Opens key:                HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprochandler32
  Opens key:                HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprochandler
  Opens key:                HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprochandler
  Opens key:                HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
  Opens key:                HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}
  Opens key:                HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}\proxystubclsid32
  Opens key:                HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}
  Opens key:                HKCR\activatableclasses\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer
  Opens key:                HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\treatas
  Opens key:                HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\treatas
  Opens key:                HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32
  Opens key:                HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}
  Opens key:                HKCR\activatableclasses\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
  Opens key:                HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
  Opens key:                HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}
  Opens key:                HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\treatas
  Opens key:                HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\treatas
  Opens key:                HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler32
  Opens key:                HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprochandler
  Opens key:                HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprochandler
  Opens key:                HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprocserver32
  Opens key:                HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprochandler32
  Opens key:                HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprochandler
  Opens key:                HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprochandler
  Opens key:                HKCU\software\microsoft\windows\currentversion\startupnotify
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\com\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key:                HKLM\software\microsoft\windowsruntime\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3}
  Opens key:                HKCR\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key:                HKCU\software\classes\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key:                HKCR\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key:                HKCU\software\classes\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3}
  Opens key:                HKCR\wow6432node\clsid\{6ae07dc1-0244-4c6f-9ab0-5017a56357c3}
  Opens key:                HKCU\software\classes\activatableclasses\clsid\{6ae07dc1-0244-4c6f-9ab0-
5017a56357c3}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}
  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\action
center\providers\eventlog\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{b447b4db-7780-11e0-ada3-18a90531a85a}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{96f4a050-7e31-453c-88be-9634f4e02139}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}
  Opens key:                HKLM\software\microsoft\windows\currentversion\action center
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6
  Opens key:                HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9
  Opens key:                 HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\persistedtsrearmed
  Opens key:                 HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\persistedsystemstate
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-12006ef9b32a
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-ba02fed39662
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0
  Opens key:                 HKLM\system\currentcontrolset\services\lanmanworkstation\parameters
  Opens key:                 HKLM\software\microsoft\rpc\extensions
  Opens key:                 HKCR\interface\{00000134-0000-0000-c000-000000000046}
  Opens key:                 HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                 HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\
  Opens key:                 HKLM\system\setup\status
  Opens key:                 HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\reboot.sl_brt_commit
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0
  Opens key:
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0
  Opens key:                 HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09
  Opens key:                 HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0
  Opens key:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_________________________________1.0.7.3_\5&34baf594&0&0.0.0
  Opens key:                 HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1
  Opens key:
HKLM\system\currentcontrolset\enum\pci\ven_80ee&dev_beef&subsys_00000000&rev_00\3&267a616a&1&10
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34\
  Opens key:                 HKLM\system\wpa\
  Opens key:                 HKLM\system\wpa\478c035f-04bc-48c7-b324-2462d786dad7-5p-9\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8\
  Opens key:                 HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9\
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}
  Opens key:                 HKCR\activatableclasses\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
  Opens key:                 HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}
  Opens key:                 HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\treatas
  Opens key:                 HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32
  Opens key:                 HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:                 HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:                 HKCU\control panel\international
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}
  Opens key:                 HKCR\activatableclasses\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
  Opens key:                 HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}
  Opens key:                 HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\treatas
  Opens key:                 HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32
  Opens key:                 HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler32
  Opens key:                 HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprochandler
  Opens key:                 HKLM\system\currentcontrolset\control\cryptography\providers
  Opens key:                 HKLM\system\currentcontrolset\control\cryptography\configuration
  Opens key:                 HKLM\software\microsoft\windowsruntime\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}
  Opens key:                 HKCR\activatableclasses\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
  Opens key:                 HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}
  Opens key:                 HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\treatas
  Opens key:                 HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32
  Opens key:                 HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler32
  Opens key:                 HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprochandler
  Opens key:                 HKLM\system\currentcontrolset\control\productoptions
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:             HKLM\system\currentcontrolset\control\nls\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
  Queries value:             HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
  Queries value:             HKLM\system\currentcontrolset\control\mui\uilanguages\en-
us[alternatecodepage]
  Queries value:             HKCU\control panel\desktop[preferreduilanguages]
  Queries value:             HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\versions[]
  Queries value:             HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[1be5bc13fd1cf615a95feec0c5b7fd13.exe]
  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\lsa\fipsalgorithmpolicy[enabled]
  Queries value:             HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:             HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
  Queries value:             HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Queries value:             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:             HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[namespace_callout]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[providerinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\windows[displayversion]
  Queries value:            HKCU\control panel\desktop[paintdesktopversion]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\setup
migration\providers\tcpip[winsock 2.0 provider id]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[type]
  Queries value:
HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft base cryptographic
provider v1.0[image path]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
  Queries value:
HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
  Queries value:            HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\setup[oobeinprogress]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\software\microsoft\rpc[idletimerwindow]
  Queries value:            HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_protocol_catalog]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[current_namespace_catalog]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000006[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000001[providerid]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0[image path]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[programdata]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist[public]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist[default]
  Queries value:            HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:            HKLM\software\microsoft\windows\currentversion[programfilesdir (x86)]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonfilesdir (x86)]
  Queries value:            HKLM\software\microsoft\windows\currentversion[programw6432dir]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonw6432dir]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
18[profileimagepath]
  Queries value:            HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
  Queries value:            HKU\.default\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[usefilter]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[debugger]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[uselargepages]
```

```
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[nodeoptions]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[disablewakecharge]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[mitigationoptions]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[disableheaplookaside]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[frontendheapdebugoptions]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[shutdownflags]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[unloadeventtracedepth]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[tracingflags]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[minimumstackcommitinbytes]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[breakoninitializeprocessfailure]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[keepactivationcontextsalive]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[trackactivationcontextreleases]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[maxdeadactivationcontexts]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[globalflag]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[cwdillegalindllsearch]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[debugprocessheaponly]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rundll32.exe[searchpathmode]
  Queries value:             HKU\.default\control panel\desktop[preferreduilanguages]
  Queries value:             HKU\.default\control
panel\desktop\muicached[machinepreferreduilanguages]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[rundll32]
  Queries value:             HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[imagepath]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[type]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[start]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[errorcontrol]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[tag]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[dependonservice]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[dependongroup]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[group]
  Queries value:             HKLM\system\currentcontrolset\services\bfe[objectname]
  Queries value:             HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\aelookupsvc\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\alluserinstallagent\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\appidsvc\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\bdesvc\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data0]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data1]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype2]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[data2]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\0[datatype3]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[action]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[type]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[guid]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data0]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data1]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype2]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[data2]
  Queries value:             HKLM\system\currentcontrolset\services\browser\triggerinfo\1[datatype3]
  Queries value:             HKLM\system\currentcontrolset\services\browser[imagepath]
  Queries value:             HKLM\system\currentcontrolset\services\browser[type]
  Queries value:             HKLM\system\currentcontrolset\services\browser[start]
  Queries value:             HKLM\system\currentcontrolset\services\browser[errorcontrol]
  Queries value:             HKLM\system\currentcontrolset\services\browser[tag]
  Queries value:             HKLM\system\currentcontrolset\services\browser[dependonservice]
  Queries value:             HKLM\system\currentcontrolset\services\browser[dependongroup]
  Queries value:             HKLM\system\currentcontrolset\services\browser[group]
  Queries value:             HKLM\system\currentcontrolset\services\browser[objectname]
  Queries value:             HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\bthserv\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\cscservice\triggerinfo\0[datatype1]
  Queries value:              HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a66e19e6]
  Queries value:              HKLM\software\microsoft\sqmclient\windows[studyid]
  Queries value:              HKLM\software\microsoft\telemetryclient\samplestore\sqm[sampledout]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\0[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[action]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[type]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[guid]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[data0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceassociationservice\triggerinfo\1[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\0[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[action]
  Queries value:              HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[type]
  Queries value:              HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[guid]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[data0]
  Queries value:
HKLM\system\currentcontrolset\services\deviceinstall\triggerinfo\1[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\dnscache\triggerinfo\0[datatype0]
  Queries value:              HKLM\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\dsmsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data1]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype2]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[data2]
  Queries value:              HKLM\system\currentcontrolset\services\dsmsvc\triggerinfo\0[datatype3]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\efs\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[action]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[type]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[guid]
  Queries value:              HKLM\system\currentcontrolset\services\fhsvc\triggerinfo\1[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\gpsvc\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\hidserv\triggerinfo\0[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[type]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\homegroupprovider\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[data0]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[imagepath]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[type]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[start]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[errorcontrol]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[tag]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[dependonservice]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[dependongroup]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[group]
  Queries value:             HKLM\system\currentcontrolset\services\ikeext[objectname]
  Queries value:             HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[data0]
  Queries value:             HKLM\system\currentcontrolset\services\keyiso\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\ktmrm\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[action]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[type]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[guid]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\1[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[action]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[type]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[guid]
  Queries value:             HKLM\system\currentcontrolset\services\lmhosts\triggerinfo\2[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[action]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[type]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[guid]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\1[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[action]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[type]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[guid]
  Queries value:             HKLM\system\currentcontrolset\services\ncasvc\triggerinfo\2[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\ncdautosetup\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\policyagent\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent[imagepath]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent[type]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent[start]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent[errorcontrol]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent[tag]
  Queries value:             HKLM\system\currentcontrolset\services\policyagent[dependonservice]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  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:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\remoteregistry\triggerinfo\0[datatype1]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[action]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[type]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[guid]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\0[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[action]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[type]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[guid]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[datatype0]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[data0]
  Queries value:             HKLM\system\currentcontrolset\services\scardsvr\triggerinfo\1[datatype1]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[conhost]
```

```
  Queries value:            HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:            HKCU\console[screencolors]
  Queries value:            HKCU\console[popupcolors]
  Queries value:            HKCU\console[insertmode]
  Queries value:            HKCU\console[quickedit]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[action]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[type]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[guid]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\0[datatype0]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[action]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[type]
  Queries value:            HKCU\console[codepage]
  Queries value:            HKCU\console[screenbuffersize]
  Queries value:            HKCU\console[windowsize]
  Queries value:            HKCU\console[windowposition]
  Queries value:            HKCU\console[fontsize]
  Queries value:            HKCU\console[fontfamily]
  Queries value:            HKCU\console[fontweight]
  Queries value:            HKCU\console[facename]
  Queries value:            HKCU\console[cursorsize]
  Queries value:            HKCU\console[historybuffersize]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[guid]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\1[datatype0]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[action]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[type]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[guid]
  Queries value:            HKLM\system\currentcontrolset\services\sensrsvc\triggerinfo\2[datatype0]
  Queries value:            HKCU\console[numberofhistorybuffers]
  Queries value:            HKCU\console[historynodup]
  Queries value:            HKCU\console[colortable00]
  Queries value:            HKCU\console[colortable01]
  Queries value:            HKCU\console[colortable02]
  Queries value:            HKCU\console[colortable03]
  Queries value:            HKCU\console[colortable04]
  Queries value:            HKCU\console[colortable05]
  Queries value:            HKCU\console[colortable06]
  Queries value:            HKCU\console[colortable07]
  Queries value:            HKCU\console[colortable08]
  Queries value:            HKCU\console[colortable09]
  Queries value:            HKCU\console[colortable10]
  Queries value:            HKCU\console[colortable11]
  Queries value:            HKCU\console[colortable12]
  Queries value:            HKCU\console[colortable13]
  Queries value:            HKCU\console[colortable14]
  Queries value:            HKCU\console[colortable15]
  Queries value:            HKCU\console[loadconime]
  Queries value:            HKCU\console[extendededitkey]
  Queries value:            HKCU\console[extendededitkeycustom]
  Queries value:            HKCU\console[worddelimiters]
  Queries value:            HKCU\console[trimleadingzeros]
  Queries value:            HKCU\console[enablecolorselection]
  Queries value:            HKCU\console[scrollscale]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[action]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[type]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[guid]
  Queries value:            HKLM\system\currentcontrolset\services\sppsvc\triggerinfo\0[datatype0]
  Queries value:            HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:            HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:            HKLM\system\currentcontrolset\control\nls\codepage\eudccoderange[1252]
  Queries value:            HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[action]
  Queries value:            HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[type]
  Queries value:            HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[guid]
  Queries value:            HKLM\system\currentcontrolset\services\storsvc\triggerinfo\0[datatype0]
  Queries value:            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[action]
  Queries value:            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[type]
  Queries value:            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[guid]
  Queries value:            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype0]
  Queries value:            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[data0]
  Queries value:            HKLM\system\currentcontrolset\services\svsvc\triggerinfo\0[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\0[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[action]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[type]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[guid]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[data0]
  Queries value:
HKLM\system\currentcontrolset\services\systemeventsbroker\triggerinfo\1[datatype1]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[action]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[type]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype0]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[data0]
  Queries value:
HKLM\system\currentcontrolset\services\tabletinputservice\triggerinfo\0[datatype1]
  Queries value:
```

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

```
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\1[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\2[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\3[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[action]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[type]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[data0]
  Queries value:
HKLM\system\currentcontrolset\services\wpdbusenum\triggerinfo\4[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[guid]
  Queries value:
HKLM\system\currentcontrolset\services\wsservice\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[action]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[type]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[guid]
  Queries value:              HKLM\system\currentcontrolset\services\wuauserv\triggerinfo\1[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[action]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[type]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[guid]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype0]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[data0]
  Queries value:              HKLM\system\currentcontrolset\services\wudfsvc\triggerinfo\0[datatype1]
  Queries value:              HKLM\system\currentcontrolset\services\wdisystemhost[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\wdisystemhost[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\wdisystemhost[wow64]
  Queries value:              HKLM\system\currentcontrolset\services\wdisystemhost[requiredprivileges]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1923240461-1905901954-2556564120-1001[profileimagepath]
  Queries value:              HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows\currentversion\explorer\user shell folders[appdata]
  Queries value:              HKU\s-1-5-21-1923240461-1905901954-2556564120-
1001\software\microsoft\windows\currentversion\explorer\user shell folders[local appdata]
  Queries value:              HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[taskhost]
  Queries value:              HKLM\software\microsoft\com3[com+enabled]
  Queries value:              HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}[]
  Queries value:              HKCR\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{900be39d-6be8-461a-bc4d-b0fa71f5ecb1}\inprocserver32[]
  Queries value:              HKCR\clsid\{900be39d-6be8-461a-bc4d-
b0fa71f5ecb1}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
a37a-4f91-bdba-fbb98fe804bf}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
a37a-4f91-bdba-fbb98fe804bf}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{15fba3b8-
a37a-4f91-bdba-fbb98fe804bf}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{282396b2-
6c46-4d66-b413-70b0445df33c}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8-e3670ed91517}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8-e3670ed91517}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{284ddb2f-
beea-4c9d-91e8-e3670ed91517}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
393e-41c3-9885-29ec5a701926}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
393e-41c3-9885-29ec5a701926}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{3ea6b3df-
393e-41c3-9885-29ec5a701926}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
10bc-4f96-9b21-4b6b83dbf476}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
10bc-4f96-9b21-4b6b83dbf476}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{45de1ea9-
10bc-4f96-9b21-4b6b83dbf476}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
fd02-4b82-a0a5-783266e430ab}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
fd02-4b82-a0a5-783266e430ab}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{4d21da64-
fd02-4b82-a0a5-783266e430ab}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
5780-49de-9eb5-8d53a51fd146}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
5780-49de-9eb5-8d53a51fd146}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{50e3b0eb-
5780-49de-9eb5-8d53a51fd146}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5c85a128-
86f7-41a4-b655-bee3f2adef46}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
398d-4edb-af71-3b830219abf7}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
```

```
398d-4edb-af71-3b830219abf7}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{5ee64afb-
398d-4edb-af71-3b830219abf7}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{63e0d0f7-
ac2f-493b-a7f2-2f3ccdb66fca}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{63e0d0f7-
ac2f-493b-a7f2-2f3ccdb66fca}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{63e0d0f7-
ac2f-493b-a7f2-2f3ccdb66fca}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
6c5b-43bb-860b-d47ae85242b1}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
6c5b-43bb-860b-d47ae85242b1}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{67f1ec80-
6c5b-43bb-860b-d47ae85242b1}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b-d429828bea2e}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b-d429828bea2e}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{72dbb5ac-
6a91-46e6-885b-d429828bea2e}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{7a54f16f-
a73a-4258-ba46-a1e998a6aa74}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{7a54f16f-
a73a-4258-ba46-a1e998a6aa74}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{7a54f16f-
a73a-4258-ba46-a1e998a6aa74}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9-
809a-482b-b60b-bcad1f8d0cd7}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9-
809a-482b-b60b-bcad1f8d0cd7}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{85e0acd9-
809a-482b-b60b-bcad1f8d0cd7}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{88d4896f-
f553-446a-9c75-9dec124ff8b7}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8cc29128-
0b57-4a2b-a7b9-a74a70ba6fa1}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8cc29128-
0b57-4a2b-a7b9-a74a70ba6fa1}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8cc29128-
0b57-4a2b-a7b9-a74a70ba6fa1}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6a50bbff5d15}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6a50bbff5d15}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{8d39bd5b-
81f8-4b94-a608-6a50bbff5d15}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{95c162b7-
5b71-44f8-82e4-abfd3108f40f}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da-
b965-4fc3-8781-88dd50a6299d}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da-
b965-4fc3-8781-88dd50a6299d}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{9c5a40da-
b965-4fc3-8781-88dd50a6299d}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
3f06-411b-9dd5-35bc5666ff3e}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
3f06-411b-9dd5-35bc5666ff3e}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a0d86e0d-
3f06-411b-9dd5-35bc5666ff3e}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
a6ca-48e0-a7c4-4cdd258439e2}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
a6ca-48e0-a7c4-4cdd258439e2}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{a59f0643-
a6ca-48e0-a7c4-4cdd258439e2}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
a840-44a9-97b1-fb74fddaa8c8}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
a840-44a9-97b1-fb74fddaa8c8}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{abd0ea66-
a840-44a9-97b1-fb74fddaa8c8}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
60e9-4301-a338-beab1c70b3e9}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
60e9-4301-a338-beab1c70b3e9}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{b171ab1c-
60e9-4301-a338-beab1c70b3e9}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a068e}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a068e}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{bf2de437-
b736-48fb-84a0-5f0c389a068e}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c0f51d84-
11b9-4e74-b083-99f11ba2db0a}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c0f51d84-
11b9-4e74-b083-99f11ba2db0a}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c0f51d84-
11b9-4e74-b083-99f11ba2db0a}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c70949f5-
bda4-4bf3-8121-af0bc174925f}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c8544339-
5be9-4f25-862e-485f1b1a6935}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c8544339-
5be9-4f25-862e-485f1b1a6935}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{c8544339-
```

```
5be9-4f25-862e-485f1b1a6935}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d6e702c0-
6c33-4657-be74-4d0c32297ba4}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{d8bcedf8-
46c3-440e-bc65-dfa6a5094054}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-
3852-4952-b76b-23bb8e35d344}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-
3852-4952-b76b-23bb8e35d344}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e4cd2e3e-
3852-4952-b76b-23bb8e35d344}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
3287-4e3f-af68-632c90f3ac95}[imagepath]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
3287-4e3f-af68-632c90f3ac95}[neverlowerpagepriority]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\diagnosticmodules\{e80cfaae-
3287-4e3f-af68-632c90f3ac95}[nameresource]
  Queries value:              HKLM\system\currentcontrolset\control\wdi\config[servername]
  Queries value:              HKLM\system\currentcontrolset\control[waittokillservicetimeout]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[17fbab0b-1e4f-45f8-
91ed-c1c85bcf6e61]
  Queries value:              HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  Queries value:
HKCU\software\microsoft\windows\currentversion\radar[clresolutioninterval]
  Queries value:              HKCU\software\microsoft\windows\currentversion\radar[displayinterval]
  Queries value:              HKCU\software\microsoft\windows\currentversion\radar[skipwatson]
  Queries value:
HKLM\software\microsoft\radar\heapleakdetection\settings[reflectioninterval]
  Queries value:              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}[]
  Queries value:              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-e212013ea917}\inprocserver32[]
  Queries value:              HKCR\clsid\{9ac9fbe1-e0a2-4ad6-b4ee-
e212013ea917}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}[]
  Queries value:              HKCR\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\inprocserver32[]
  Queries value:              HKCR\clsid\{c90250f3-4d7d-4991-9b69-
a5c5bc1c2ae6}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{dbea162d-04e8-460f-8a0b-4a431715d9a3}\proxystubclsid32[]
  Queries value:              HKCR\interface\{92ca9dcd-5622-4bba-a805-5e9f541bd8c9}\proxystubclsid32[]
  Queries value:              HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}[]
  Queries value:              HKCR\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{603d3801-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[]
  Queries value:              HKCR\clsid\{603d3801-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32[threadingmodel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[typeahead]
  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\eventsystem[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\bits[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\bits[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\bits[wow64]
  Queries value:              HKLM\system\currentcontrolset\services\bits[requiredprivileges]
  Queries value:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues[capabilities]
  Queries value:
HKLM\system\currentcontrolset\enum\swd\printenum\printqueues[configflags]
  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:              HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[segoe
ui]
  Queries value:              HKCU\control panel\desktop[caretwidth]
  Queries value:              HKCU\control panel\desktop[cursorblinkrate]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[alwaysshowmenus]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[alwaysshowmenus]
  Queries value:              HKCU\software\microsoft\internet explorer\toolbar[menuuserexpanded]
  Queries value:              HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}[]
  Queries value:              HKCR\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{f5a8b627-4d46-4d65-92f3-73626ae31971}\inprocserver32[]
  Queries value:              HKCR\clsid\{f5a8b627-4d46-4d65-92f3-
73626ae31971}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[explorercommandhandler]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[impliedselectionmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[folderhandler]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[invokecommandonselection]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[sendtoverb]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[opencontrolpanel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[opencontrolpanelpage]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\commandstore\shell\windows.statusbar[panevisibleproperty]
  Queries value:
```

```
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showstatusbar]
  Queries value:              HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}[]
  Queries value:              HKCR\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{b77b1cbf-e827-44a9-a33a-6ccfeeaa142a}\inprocserver32[]
  Queries value:              HKCR\clsid\{b77b1cbf-e827-44a9-a33a-
6ccfeeaa142a}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}[]
  Queries value:              HKCR\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{76765b11-3f95-4af2-ac9d-ea55d8994f1a}\inprocserver32[]
  Queries value:              HKCR\clsid\{76765b11-3f95-4af2-ac9d-
ea55d8994f1a}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}[system.proplist.statusbar]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{26dc287c-6e3d-4bd3-
b2b0-6a26ba2e346d} 4]
  Queries value:              HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}[]
  Queries value:              HKCR\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{b8967f85-58ae-4f46-9fb2-5d7904798f4b}\inprocserver32[]
  Queries value:              HKCR\clsid\{b8967f85-58ae-4f46-9fb2-
5d7904798f4b}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[system.statusicons]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{7a55582b-bd8c-4475-
b94c-b87a388a7899} 100]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-
e946b44c8dd5}[system.librarylocationscount]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{908696c7-8f87-44f2-
80ed-a8c1c6894575} 2]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[system.sync.itemstate]
  Queries value:              HKCR\clsid\{031e4825-7b94-4dc3-b131-e946b44c8dd5}[{7bd5533e-af15-44db-
b8c8-bd6624e1d032} 25]
  Queries value:              HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffff_ffffffff_0^cc77560bc3634a486857716562968286[timestamp]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_1414_008d_ffffffff_ffffffff_0^cc77560bc3634a486857716562968286[setid]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14[timestamp]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14[setid]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\connectivity\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14[recent]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_ryi0001 agnieszka
01_1d_07d7_b2_1414_008d_ffffffff_ffffffff_0^700ef59a5da31cbd79f31237af2ad4c4[timestamp]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msh062e0_00_07db_c6^182fdc0875f0a76803e4a9848a8c1ea7[timestamp]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[primsurfsize.cx]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[primsurfsize.cy]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[stride]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[pixelformat]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[colorbasis]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[position.cx]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00[position.cy]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[flags]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[videostandard]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[activesize.cx]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[activesize.cy]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[vsyncfreq.numerator]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[vsyncfreq.denominator]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[hsyncfreq.numerator]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[hsyncfreq.denominator]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[pixelrate]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[scanlineordering]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[scaling]
  Queries value:
HKLM\system\currentcontrolset\control\graphicsdrivers\configuration\msbdd_noedid_80ee_beef_00000000_00020000_0^ab02a9ab10912b3b7f8c017a344c8d14\00\00[rotation]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[notaskgrouping]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbarglomlevel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbaranimations]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[taskbarsmallicons]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[taskbarsmallicons]
  Queries value:              HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}[capabilities]
  Queries value:              HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}[configflags]
  Queries value:              HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en]
  Queries value:              HKLM\system\currentcontrolset\control\devicecontainers\{623cc954-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[]
  Queries value:              HKLM\system\currentcontrolset\enum\swd\printenum\{af023001-e0b1-4934-
b8e8-d92d736469be}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011[]
  Queries value:              HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}[capabilities]
  Queries value:              HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}[configflags]
  Queries value:              HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en-us]
  Queries value:              HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[en]
  Queries value:              HKLM\system\currentcontrolset\control\devicecontainers\{623cc955-8780-
11e3-be67-0800272f6e60}\properties\{3464f7a4-2444-40b1-980a-e0903cb6d912}\000a[]
  Queries value:              HKLM\system\currentcontrolset\enum\swd\printenum\{8b164225-43e2-473f-
b32c-cd2da77617c7}\properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0011[]
  Queries value:              HKCR\clsid\{21ec2020-3aea-1069-a2dd-08002b30309d}[sortorderindex]
  Queries value:              HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[attributes]
  Queries value:              HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}[]
  Queries value:              HKCR\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{317d06e8-5f24-433d-bdf7-79ce68d8abc2}\inprocserver32[]
  Queries value:              HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[callforattributes]
  Queries value:              HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[restrictedattributes]
  Queries value:              HKCR\clsid\{21ec2020-3aea-1069-a2dd-
08002b30309d}\shellfolder[foldervalueflags]
  Queries value:              HKCR\clsid\{317d06e8-5f24-433d-bdf7-
79ce68d8abc2}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{21ec2020-3aea-1069-a2dd-
08002b30309d}]
  Queries value:              HKCR\clsid\{35786d3c-b075-49b9-88dd-029876e11c01}[sortorderindex]
  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\{289af617-
1cc3-42a6-926c-e6a863f0e3ba}[suppressionpolicy]
  Queries value:              HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}[]
  Queries value:              HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{6f13dd2e-ebee-4dd5-a72e-850b2087f5dd}\inprocserver32[]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\mycomputer\namespace\delegatefolders\{35786d3c-
b075-49b9-88dd-029876e11c01}[suppressionpolicy]
  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\{6f13dd2e-ebee-4dd5-a72e-
850b2087f5dd}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf}[sortorderindex]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[attributes]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[callforattributes]
  Queries value:
HKLM\software\microsoft\windows\currentversion\photopropertyhandler\containerassociations[{57a37caa-
367a-4540-916b-f183c5093a4b}]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[restrictedattributes]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[foldervalueflags]
  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:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[enablethumbnails]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[nodefaulttofs]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[parsedisplaynameneedsurl]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[blocknewfile]
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[noinitrequired]
```

```
  Queries value:              HKCR\clsid\{9c73f5e5-7ae7-4e32-a8e8-
8d23b85255bf}\shellfolder[saferootformta]
  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:              HKCU\software\microsoft\windows\currentversion\shell
extensions\cached[{9c73f5e5-7ae7-4e32-a8e8-8d23b85255bf} {000214e6-0000-0000-c000-000000000046}
0xffff]
  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:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{d5291c64-7c88-
11e3-be65-806e6f6e6963}[generation]
  Queries value:              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders[suppressionpolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders[]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\userslibraries\namespace\delegatefolders\{896664f7-
12e1-490f-8782-c0835afd98fc}[suppressionpolicy]
  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:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[system.namespaceclsid]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{28636aa6-953d-11d2-
b5d6-00c04fd918d0} 6]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}[system.ispinnedtonamespacetree]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[{5d76b67f-9b3d-44bb-
b6ae-25da4f638a67} 2]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\defaulticon[]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}\defaulticon[openicon]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\clsid\{20d04fe0-
3aea-1069-a2d8-08002b30309d}[]
  Queries value:              HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}[localizedstring]
  Queries value:              HKLM\system\currentcontrolset\services\bits[type]
  Queries value:              HKLM\system\currentcontrolset\services\bits[start]
  Queries value:              HKLM\system\currentcontrolset\services\bits[errorcontrol]
  Queries value:              HKLM\system\currentcontrolset\services\bits[tag]
  Queries value:              HKLM\system\currentcontrolset\services\bits[dependonservice]
  Queries value:              HKLM\system\currentcontrolset\services\bits[dependongroup]
  Queries value:              HKLM\system\currentcontrolset\services\bits[group]
  Queries value:              HKLM\system\currentcontrolset\services\http[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\ssdpsrv[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\ssdpsrv[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\ssdpsrv[wow64]
  Queries value:              HKLM\system\currentcontrolset\services\ssdpsrv[requiredprivileges]
  Queries value:              HKLM\system\currentcontrolset\services\sppsvc[objectname]
  Queries value:              HKLM\system\currentcontrolset\services\sppsvc[imagepath]
  Queries value:              HKLM\system\currentcontrolset\services\sppsvc[wow64]
  Queries value:              HKLM\system\currentcontrolset\services\sppsvc[requiredprivileges]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-
20[profileimagepath]
  Queries value:              HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[appdata]
  Queries value:              HKU\s-1-5-20\software\microsoft\windows\currentversion\explorer\user
shell folders[local appdata]
  Queries value:              HKLM\system\currentcontrolset\services\sppsvc[environment]
  Queries value:              HKLM\system\currentcontrolset\services\sppsvc[startprotected]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[sppsvc]
  Queries value:              HKLM\system\currentcontrolset\control\mui\settings[preferreduilanguages]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[e23b33b0-c8c9-472c-
a5f9-f2bdfea0f156]
  Queries value:              HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}[]
  Queries value:              HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-323e85a1ce84}\inprocserver32[]
  Queries value:              HKCR\clsid\{9dac2c1e-7c5c-40eb-833b-
323e85a1ce84}\inprocserver32[threadingmodel]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[1b0ac240-cbb8-4d55-
8539-9230a44081a5]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[5857d6ca-9732-4454-
809b-2a87b70881f8]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[9dac2c1e-7c5c-40eb-
833b-323e85a1ce84]
  Queries value:              HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:              HKLM\software\policies\microsoft\internet
explorer\security[disablefixsecuritysettings]
  Queries value:              HKCU\software\microsoft\internet
explorer\security[disablefixsecuritysettings]
  Queries value:              HKLM\software\microsoft\internet
explorer\security[disablefixsecuritysettings]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.101[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.103[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.100[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.102[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.104[checksetting]
  Queries value:              HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}[]
  Queries value:              HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{ca236752-2e77-4386-b63b-0e34774a413d}\inprocserver32[]
  Queries value:              HKCR\clsid\{ca236752-2e77-4386-b63b-
0e34774a413d}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[a0ef609d-0a14-424c-
9270-3b2691a0a394]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[3e19a300-75d9-4027-
86ba-948b70416220]
  Queries value:              HKLM\software\microsoft\windows\windows error reporting[disabled]
  Queries value:              HKCU\software\microsoft\windows\windows error reporting[disabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:              HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}[]
  Queries value:              HKCR\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{88d96a05-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value:              HKCR\clsid\{88d96a05-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
  Queries value:              HKCU\software\microsoft\windows\windows error
reporting[lastqueuepestertime]
  Queries value:              HKLM\software\microsoft\windows\windows error
reporting[queuepesterinterval]
  Queries value:              HKCU\software\microsoft\windows\windows error
reporting[queuepesterinterval]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101[checksetting]
  Queries value:              HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}[]
  Queries value:              HKCR\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{c8e6f269-b90a-4053-a3be-499afcec98c4}\inprocserver32[]
  Queries value:              HKCR\clsid\{c8e6f269-b90a-4053-a3be-
499afcec98c4}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\system[enablelua]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0[checksetting]
  Queries value:              HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}[]
  Queries value:              HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}[]
  Queries value:              HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{900c0763-5cad-4a34-bc1f-40cd513679d5}\inprocserver32[]
  Queries value:              HKCR\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}\inprocserver32[]
  Queries value:              HKCR\clsid\{900c0763-5cad-4a34-bc1f-
40cd513679d5}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{088e8dfb-2464-4c21-bad2-
f0aa6db5d4bc}\inprocserver32[threadingmodel]
  Queries value:              HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
  Queries value:              HKLM\software\policies\microsoft\windows\system[enablesmartscreen]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer[smartscreenenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}[]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}\inprocserver32[]
  Queries value:              HKCR\clsid\{a4a1a128-768f-41e0-bf75-
e4fddd701cba}\inprocserver32[threadingmodel]
  Queries value:              HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}[]
  Queries value:              HKCR\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{d26de5c1-c061-43f7-9c40-7517526cf1c1}\inprocserver32[]
  Queries value:              HKCR\clsid\{d26de5c1-c061-43f7-9c40-
7517526cf1c1}\inprocserver32[threadingmodel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\startupnotify[enablestartupappnotification]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{01979c6a-42fa-414c-b8aa-eee2c8202018}[lastknownstate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{dab69a6a-4d2a-4d44-94bf-e0091898c881}[lastknownstate]
  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:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{de7b24ea-73c8-4a09-985d-5bdadcfa9017}.check.800[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{134ea407-755d-4a93-b8a6-f290cd155023}[lastknownstate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{134ea407-755d-4a93-b8a6-f290cd155023}.check.8001[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{c4efc9bb-2570-4821-8923-1bad317d2d4b}[lastknownstate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{c4efc9bb-2570-4821-8923-1bad317d2d4b}.check.100[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{b447b4db-7780-11e0-ada3-18a90531a85a}.check.100[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{3ff37a1c-a68d-4d6e-8c9b-f79e8b16c482}.check.100[checksetting]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{2374911b-b114-42fe-900d-54f95fee92e5}[lastknownstate]
  Queries value:              HKCU\software\microsoft\windows\currentversion\action
center\checks\{2374911b-b114-42fe-900d-54f95fee92e5}.check.100[checksetting]
```

```
  Queries value:           HKCU\software\microsoft\windows\currentversion\action
center\checks\{96f4a050-7e31-453c-88be-9634f4e02139}.check.8010[checksetting]
  Queries value:           HKCU\software\microsoft\windows\currentversion\action
center\providers\eventlog\{aa4c798d-d91b-4b07-a013-787f5803d6fc}[lastknownstate]
  Queries value:           HKCU\software\microsoft\windows\currentversion\action
center\checks\{aa4c798d-d91b-4b07-a013-787f5803d6fc}.check.100[checksetting]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[inactivityshutdowndelay]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[keeprunningthresholdmins]
  Queries value:           HKLM\system\currentcontrolset\services\wsearch[objectname]
  Queries value:           HKLM\system\currentcontrolset\services\wmpnetworksvc[objectname]
  Queries value:           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[tokenstore]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-1[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-10[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-11[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-12[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-13[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-14[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-15[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-16[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-17[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-18[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-19[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-2[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-20[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-21[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-22[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-23[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-24[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-25[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-26[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-27[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-28[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-29[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-3[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-30[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-31[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-32[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-33[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-4[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-5[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-6[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-7[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-8[]
  Queries value:           HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-9[]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
12006ef9b32a[manifestfile]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\179b8a65-b0f6-41d9-acea-
12006ef9b32a[pluginfile]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-
ba02fed39662[manifestfile]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\modules\c42d83ff-5958-4af4-a0dd-
ba02fed39662[pluginfile]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/bios/4.0[isservice]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[moduleid]
  Queries value:           HKLM\software\microsoft\windows
```

```
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[moduleid]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/windowsfunctionality/agent/7.0[isservice]
  Queries value:
HKLM\system\currentcontrolset\services\lanmanworkstation\parameters[rpccachetimeout]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/activedirectory/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/flags/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/hwid/4.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/phone/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2005[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/2009[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/pkey/detect[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/vmd/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:rm/algorithm/volume/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/createprocess/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/kernel/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/reeval/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/action/vlactivate/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/actionscheduler/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/apihandler/object/activedirectorypublisher/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/global/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/collector/kms/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/eul/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pa/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/pkc/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/rac/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/payloadhandler/spc/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/licenseacquisition/sequence/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/statecollector/pkey[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/taskscheduler/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/1.0[isservice]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform\plugins\objects\msft:spp/volume/services/kms/activationinfo/1.0[isservice]
  Queries value:              HKLM\software\microsoft\rpc\extensions[ndroleextdll]
  Queries value:              HKLM\software\microsoft\com3[finalizeractivitybypass]
  Queries value:              HKCR\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32[]
  Queries value:              HKCU\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[kmshostconfig]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[enabletestvolumeintervals]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[vlactivationinterval]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[vlrenewalinterval]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[actionlist]
  Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[publisherpolicychangetime]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[cachestore]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion[digitalproductid4]
  Queries value:              HKLM\system\setup\status[auditboot]
  Queries value:              HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[hardwareid]
  Queries value:              HKLM\system\currentcontrolset\enum\acpi\pnp0a03\0[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_1237&subsys_00000000&rev_02\3&267a616a&1&00[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7000&subsys_00000000&rev_00\3&267a616a&1&08[compatibleids]
  Queries value:              HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0303\4&e03a844&0[compatibleids]
  Queries value:              HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0200\4&e03a844&0[compatibleids]
  Queries value:              HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0f03\4&e03a844&0[compatibleids]
  Queries value:              HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0400\4&e03a844&0[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\lptenum\microsoftrawport\5&2539bd28&0&lpt1[compatibleids]
  Queries value:            HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0100\4&e03a844&0[compatibleids]
  Queries value:            HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\acpi\pnp0000\4&e03a844&0[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\pci\ven_8086&dev_7111&subsys_00000000&rev_01\3&267a616a&1&09[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&0[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_________________________________1.0.7.3_\5&34baf594&0&0.0.0[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\ide\diskhitachi_________________________________1.0.7.3_\5&34baf594&0&0.0.0[compatibleids]
  Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[hardwareid]
  Queries value:
HKLM\system\currentcontrolset\enum\pciide\idechannel\4&20064fa2&0&1[compatibleids]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[licstatusarray]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[policyvaluesarray]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[hasooberun]
  Queries value:            HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}[]
  Queries value:            HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{88d96a06-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value:            HKCR\clsid\{88d96a06-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
  Queries value:            HKCU\control panel\international[scurrencyoverride]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[servicesessionid]
  Queries value:            HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}[]
  Queries value:            HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{88d96a08-f192-11d4-a65f-0040963251e5}\inprocserver32[]
  Queries value:            HKCR\clsid\{88d96a08-f192-11d4-a65f-
0040963251e5}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[logcontext]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}[]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}\inprocserver32[]
  Queries value:            HKCR\clsid\{0f87369f-a4e5-4cfc-bd3e-
73e6154572dd}\inprocserver32[threadingmodel]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[productpolicy]
  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:       HKLM\system\wpa\8dec0af1-0341-4b93-85cd-72606c2df94c-6p-34[]
  Value changes:            HKCR\clsid\{5839fca9-774d-42a1-acda-d6a79037f57f}\inprocserver32[]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000010[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000009[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000008[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000007[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000006[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000005[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000004[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000003[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000002[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries64\000000000001[packedcatalogitem]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000005[librarypath]
```

```
  Value changes:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries64\000000000004[librarypath]
  Value changes:            HKLM\system\currentcontrolset\services\browser[start]
  Value changes:            HKLM\system\currentcontrolset\services\policyagent[start]
  Value changes:            HKCU\software\microsoft\internet
explorer\toolbar\shellbrowser[itbar7layout]
  Value changes:            HKCU\software\microsoft\windows\currentversion\action
center\checks\{e8433b72-5842-4d43-8645-bc2c35960837}.check.106[checksetting]
  Value changes:            HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.100[checksetting]
  Value changes:            HKCU\software\microsoft\windows\currentversion\action
center\checks\{852fb1f8-5cc6-4567-9c0e-7c330f8807c2}.check.101[checksetting]
  Value changes:            HKCU\software\microsoft\windows\currentversion\action
center\checks\{088e8dfb-2464-4c21-bad2-f0aa6db5d4bc}.check.0[checksetting]
  Value changes:            HKCU\software\microsoft\windows\currentversion\action
center\checks\{d26de5c1-c061-43f7-9c40-7517526cf1c1}.check.0[checksetting]
  Value changes:            HKCU\software\microsoft\windows\currentversion\action
center\checks\{c8e6f269-b90a-4053-a3be-499afcec98c4}.check.0[checksetting]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[servicesessionid]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[licstatusarray]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\softwareprotectionplatform[actionlist]
```