Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	804
Risk Level:	10
Date Processed:	2016-05-18 10:40:23 (UTC)
Processing Time:	63.05 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0fe92a59448dcd7b0d7f239c237a351e.exe"
Sample ID:	3324
Type:	basic
Owner:	admin
Label:	0fe92a59448dcd7b0d7f239c237a351e
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui:.net
File Size:	44544 bytes
MD5:	0fe92a59448dcd7b0d7f239c237a351e
SHA256:	5bf14321c62ae838db535affdb9ef20949c61ee3816a222e3f610b384feaca43
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
3	Long sleep detected
2	.NET compiled executable
5	Installs service
10	Creates malicious events: Bladabindi 2 [Backdoor, RAT]
10	Creates malicious events: Bladabindi [Backdoor, RAT]
5	Creates process in suspicious location
7	Attempts to connect to dynamic DNS
6	Checks Network Access Protection parameters
4	Reads process memory
5	Modifies firewall policy
6	Modifies firewall
5	Adds autostart object
4	Terminates process under Windows subfolder

Process/Thread Events

```
  Creates process:         C:\WINDOWS\Temp\0fe92a59448dcd7b0d7f239c237a351e.exe
["c:\windows\temp\0fe92a59448dcd7b0d7f239c237a351e.exe" ]
  Creates process:         C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe
["C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe" ]
  Creates process:         C:\WINDOWS\system32\netsh.exe [netsh firewall add allowedprogram
"C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe" "Trojan.exe" ENABLE]
  Reads from process:      PID:1956 C:\Program Files\Java\jre7\bin\jqs.exe
  Reads from process:      PID:1416 C:\WINDOWS\system32\rundll32.exe
  Reads from process:      PID:1148 C:\WINDOWS\system32\svchost.exe
  Reads from process:      PID:344 C:\WINDOWS\system32\netsh.exe
  Reads from process:      PID:1840 C:\WINDOWS\system32\wbem\unsecapp.exe
  Reads from process:      PID:592 C:\WINDOWS\system32\winlogon.exe
  Reads from process:      PID:1208 C:\WINDOWS\system32\alg.exe
  Reads from process:      PID:1732 C:\WINDOWS\system32\spoolsv.exe
  Reads from process:      PID:1068 C:\WINDOWS\system32\svchost.exe
  Reads from process:      PID:388 C:\WINDOWS\system32\smss.exe
  Reads from process:      PID:564 C:\WINDOWS\system32\csrss.exe
  Reads from process:      PID:1896 C:\WINDOWS\explorer.exe
  Reads from process:      PID:1272 C:\WINDOWS\system32\svchost.exe
  Reads from process:      PID:292 C:\WINDOWS\system32\ctfmon.exe
  Reads from process:      PID:540 C:\WINDOWS\system32\wbem\wmiprvse.exe
  Reads from process:      PID:908 C:\WINDOWS\system32\lsass.exe
  Reads from process:      PID:272 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
  Reads from process:      PID:896 C:\WINDOWS\system32\services.exe
  Reads from process:      PID:1340 C:\WINDOWS\system32\svchost.exe
  Terminates process:      C:\WINDOWS\Temp\0fe92a59448dcd7b0d7f239c237a351e.exe
  Terminates process:      C:\WINDOWS\system32\netsh.exe
```

Named Object Events

```
  Creates mutex:           \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
  Creates mutex:           \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
  Creates mutex:           \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
  Creates mutex:           \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
  Creates mutex:           \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-
1957994488-1003
  Creates mutex:           \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-
507921405-1957994488-1003MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
  Creates mutex:           \BaseNamedObjects\ZonesCounterMutex
  Creates mutex:           \BaseNamedObjects\ZoneAttributeCacheCounterMutex
  Creates mutex:           \BaseNamedObjects\ZonesCacheCounterMutex
  Creates mutex:           \BaseNamedObjects\ZonesLockedCacheCounterMutex
  Creates mutex:         \BaseNamedObjects\SHIMLIB_LOG_MUTEX
  Creates mutex:         \BaseNamedObjects\5cd8f17f4086744065eb0992a09e05a2
  Creates mutex:         \BaseNamedObjects\.net clr networking
  Creates event:         \BaseNamedObjects\CorDBIPCSetupSyncEvent_300
  Creates event:         \BaseNamedObjects\CorDBIPCSetupSyncEvent_304
  Creates event:         \BaseNamedObjects\userenv: User Profile setup event
  Creates semaphore:     \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
  Creates semaphore:     \BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
  Creates semaphore:     \BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
```

File System Events

```
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe
  Creates:               C:\Documents and Settings\Admin\Start
Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
  Creates:               C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe.tmp
  Opens:                 C:\WINDOWS\Prefetch\0FE92A59448DCD7B0D7F239C237A3-39AB25B2.pf
  Opens:                 C:\Documents and Settings\Admin
  Opens:                 C:\WINDOWS\system32\mscoree.dll
  Opens:                 C:\WINDOWS\system32\imm32.dll
  Opens:                 C:\windows\temp\0fe92a59448dcd7b0d7f239c237a351e.exe.config
  Opens:                 C:\WINDOWS\Temp\0fe92a59448dcd7b0d7f239c237a351e.exe
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Manifest
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll.2.Config
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca
  Opens:
C:\WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-
ww_b80fa8ca\msvcr80.dll
  Opens:                 C:\
  Opens:                 C:\WINDOWS
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
  Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
  Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
  Opens:                 C:\WINDOWS\system32\shell32.dll
  Opens:                 C:\WINDOWS\system32\shell32.dll.124.Manifest
  Opens:                 C:\WINDOWS\system32\shell32.dll.124.Config
  Opens:                 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                 C:\WINDOWS\WindowsShell.Manifest
  Opens:                 C:\WINDOWS\WindowsShell.Config
  Opens:                 C:\WINDOWS\system32\comctl32.dll
  Opens:                 C:\WINDOWS\system32\comctl32.dll.124.Manifest
  Opens:                 C:\WINDOWS\system32\comctl32.dll.124.Config
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
Config\v2.0.50727.42\security.config
  Opens:                 C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
Config\v2.0.50727.42\security.config.cch
  Opens:                 C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\index9c.dat
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\mscorlib\9adb89fa22fd5b4ce433b5aca7fb1b07\mscorlib.ni.dll
  Opens:                 C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089
  Opens:                 C:\WINDOWS\Temp
  Opens:                 C:\WINDOWS\system32\rpcss.dll
  Opens:                 C:\WINDOWS\system32\MSCTF.dll
  Opens:                 C:\WINDOWS\system32\l_intl.nls
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Manifest
  Opens:                 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll.2.Config
  Opens:                 C:\WINDOWS\assembly\pubpol1.dat
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System\aa7926460a336408c8041330ad90929d\System.ni.dll
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\5b3d048d8c003d743ea5e72caf07773a\Microsoft.VisualBasic.ni.dll
  Opens:
C:\WINDOWS\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0__b03f5f7f11d50a3a
  Opens:                 C:\WINDOWS\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Drawing\6978f2e90f13bc720d57fa6895c911e2\System.Drawing.ni.dll
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\9a254c455892c02355ab0ab0f0727c5b\System.Windows.Forms.ni.dll
  Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089
  Opens:                 C:\WINDOWS\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a
  Opens:
C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
  Opens:
C:\WINDOWS\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
  Opens:                 C:\Documents and Settings
  Opens:                 C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                    C:\WINDOWS\system32\netapi32.dll
  Opens:                    C:\WINDOWS\system32\setupapi.dll
  Opens:                    C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:                    C:\Documents and Settings\All Users
  Opens:                    C:\Documents and Settings\All Users\Documents\desktop.ini
  Opens:                    C:\WINDOWS\system32\clbcatq.dll
  Opens:                    C:\WINDOWS\system32\comres.dll
  Opens:                    C:\WINDOWS\Registration\R000000000007.clb
  Opens:                    C:\WINDOWS\system32\urlmon.dll
  Opens:                    C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:                    C:\Documents and Settings\Admin\Local Settings
  Opens:                    C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe
  Opens:                    C:\WINDOWS\system32\apphelp.dll
  Opens:                    C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                    C:\WINDOWS\AppPatch\systest.sdb
  Opens:                    C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe.Manifest
  Opens:                    C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe.Config
  Opens:                    C:\WINDOWS\Prefetch\TROJAN.EXE-24702E36.pf
  Opens:                    C:\DOCUME~1\Admin\LOCALS~1\Temp\Trojan.exe.config
  Opens:                    C:\WINDOWS\system32\winlogon.exe
  Opens:                    C:\WINDOWS\system32\xpsp2res.dll
  Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch.300.64803
  Opens:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch.300.64803
  Opens:                    C:\Documents and Settings\Admin\Application Data\Microsoft\CLR Security
Config\v2.0.50727.42\security.config.cch.300.64833
  Opens:                    C:\WINDOWS\system32\netsh.exe
  Opens:                    C:\WINDOWS\system32
  Opens:                    C:\WINDOWS\system32\netsh.exe.Manifest
  Opens:                    C:\WINDOWS\Prefetch\NETSH.EXE-085CFFDE.pf
  Opens:                    C:\WINDOWS\system32\shfolder.dll
  Opens:                    C:\WINDOWS\system32\mprapi.dll
  Opens:                    C:\WINDOWS\system32\activeds.dll
  Opens:                    C:\Documents and Settings\Admin\Start Menu\Programs\Startup
  Opens:                    C:\WINDOWS\system32\adsldpc.dll
  Opens:                    C:\WINDOWS\system32\atl.dll
  Opens:                    C:\WINDOWS\system32\rtutils.dll
  Opens:                    C:\WINDOWS\system32\samlib.dll
  Opens:                    C:\WINDOWS\system32\rasapi32.dll
  Opens:                    C:\WINDOWS\system32\rasman.dll
  Opens:                    C:\WINDOWS\system32\ws2_32.dll
  Opens:                    C:\WINDOWS\system32\ws2help.dll
  Opens:                    C:\WINDOWS\system32\tapi32.dll
  Opens:                    C:\WINDOWS\system32\winmm.dll
  Opens:                    C:\WINDOWS\system32\iphlpapi.dll
  Opens:                    C:\WINDOWS\system32\shimeng.dll
  Opens:                    C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:                    C:\WINDOWS\system32\msacm32.dll
  Opens:                    C:\WINDOWS\system32\uxtheme.dll
  Opens:                    C:\WINDOWS\system32\TAPI32.dll.124.Manifest
  Opens:                    C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:                    C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:                    C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:                    C:\WINDOWS\system32\ipv6mon.dll
  Opens:                    C:\WINDOWS\system32\xpob2res.dll
  Opens:                    C:\WINDOWS\system32\ipmontr.dll
  Opens:                    C:\WINDOWS\system32\ifmon.dll
  Opens:                    C:\WINDOWS\system32\netcfgx.dll
  Opens:                    C:\WINDOWS\system32\clusapi.dll
  Opens:                    C:\WINDOWS\system32\dnsapi.dll
  Opens:                    C:\WINDOWS\system32\netshell.dll
  Opens:                    C:\WINDOWS\system32\credui.dll
  Opens:                    C:\WINDOWS\system32\dot3api.dll
  Opens:                    C:\WINDOWS\system32\dot3dlg.dll
  Opens:                    C:\WINDOWS\system32\onex.dll
  Opens:                    C:\WINDOWS\system32\wtsapi32.dll
  Opens:                    C:\WINDOWS\system32\winsta.dll
  Opens:                    C:\WINDOWS\system32\crypt32.dll
  Opens:                    C:\WINDOWS\system32\msasn1.dll
  Opens:                    C:\WINDOWS\system32\eappcfg.dll
  Opens:                    C:\WINDOWS\system32\msvcp60.dll
  Opens:                    C:\WINDOWS\system32\eappprxy.dll
  Opens:                    C:\WINDOWS\system32\mswsock.dll
  Opens:                    C:\WINDOWS\system32\psapi.dll
  Opens:                    C:\WINDOWS\system32\netshell.dll.50.Manifest
  Opens:                    C:\WINDOWS\system32\netshell.dll.50.Config
  Opens:                    C:\WINDOWS\system32\ippromon.dll
  Opens:                    C:\WINDOWS\system32\rasmontr.dll
  Opens:                    C:\WINDOWS\system32\ipxmontr.dll
  Opens:                    C:\WINDOWS\system32\ipxpromn.dll
  Opens:                    C:\WINDOWS\system32\dgnet.dll
  Opens:                    C:\WINDOWS\system32\wbem\framedyn.dll
  Opens:                    C:\WINDOWS\system32\wbem\wbemprox.dll
  Opens:                    C:\WINDOWS\system32\wbem\wbemcomn.dll
  Opens:                    C:\WINDOWS\system32\hnetmon.dll
  Opens:                    C:\WINDOWS\system32\fwcfg.dll
  Opens:                   C:\WINDOWS\system32\napmontr.dll
  Opens:                   C:\WINDOWS\system32\qutil.dll
  Opens:                   C:\WINDOWS\system32\dot3cfg.dll
  Opens:                   C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe.tmp
  Opens:                   C:\WINDOWS\system32\qagent.dll
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Configuration\cb4cb21d14767292e079366a5d3d76cd\System.Configuration.ni.dll
  Opens:                   C:\WINDOWS\system32\wbem\wbemsvc.dll
  Opens:                   C:\WINDOWS\system32\wbem\fastprox.dll
  Opens:                   C:\WINDOWS\system32\ntdsapi.dll
  Opens:
C:\WINDOWS\assembly\GAC_MSIL\System.Configuration\2.0.0.0__b03f5f7f11d50a3a
  Opens:
C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\System.Xml\36f3953f24d4f0b767bf172331ad6f3e\System.Xml.ni.dll
  Opens:                   C:\WINDOWS\assembly\GAC_MSIL\System.Xml\2.0.0.0__b77a5c561934e089
  Opens:                   C:\WINDOWS\Temp\d39cb9f7-780e-4439-9461-4f41bca9b7b3
  Opens:                   C:\WINDOWS\system32\hnetcfg.dll
  Opens:                   C:\WINDOWS\system32\wshtcpip.dll
  Opens:                   C:\WINDOWS\system32\drivers\etc\hosts
  Opens:                   C:\WINDOWS\system32\rsaenh.dll
  Opens:                   C:\WINDOWS\system32\rasadhlp.dll
  Writes to:               C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe
  Writes to:               C:\Documents and Settings\Admin\Start
Menu\Programs\Startup\5cd8f17f4086744065eb0992a09e05a2.exe
  Writes to:               C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe.tmp
  Reads from:              C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
  Reads from:              C:\Documents and Settings\Admin\My Documents\desktop.ini
  Reads from:              C:\Documents and Settings\All Users\Documents\desktop.ini
  Reads from:              C:\WINDOWS\Registration\R000000000007.clb
  Reads from:              C:\Documents and Settings\Admin\Local Settings\Temp\Trojan.exe
  Reads from:              C:\WINDOWS\system32\drivers\etc\hosts
  Reads from:              C:\WINDOWS\system32\rsaenh.dll
```

Network Events

```
  DNS query:               almashaks70.no-ip.org
  Sends data to:           8.8.8.8:53
  Receives data from:      0.0.0.0:0
```

Windows Registry Events

```
  Creates key:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:             HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:             HKLM\software\microsoft\fusion\gacchangenotification\default
  Creates key:             HKCU\software\5cd8f17f4086744065eb0992a09e05a2
  Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}\
  Creates key:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:             HKLM\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:             HKCU\software\microsoft\multimedia\audio
  Creates key:             HKCU\software\microsoft\multimedia\audio compression manager\
  Creates key:             HKCU\software\microsoft\multimedia\audio compression manager\msacm
  Creates key:             HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00
  Creates key:             HKLM\system\currentcontrolset\services\tcpip\parameters
  Creates key:             HKLM\software\microsoft\windows nt\currentversion\tracing
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy\traceidentifier
  Creates key:             HKLM\software\microsoft\wbem\cimom
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil\traceidentifier
  Creates key:             HKLM\software\microsoft\tracing
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh\napmontr
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent
  Creates key:             HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent\traceidentifier
  Creates key:             HKLM\system\currentcontrolset\services\napagent\localconfig
  Creates key:
HKLM\system\currentcontrolset\services\napagent\localconfig\enroll\hcsgroups
  Creates key:             HKLM\system\currentcontrolset\services\napagent\shas
  Creates key:             HKLM\system\currentcontrolset\services\napagent\qecs
  Creates key:             HKLM\system\currentcontrolset\services\napagent\localconfig\ui
  Creates key:
```

```
HKLM\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\0fe92a59448dcd7b0d7f239c237a351e.exe
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscoree.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\.netframework
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKCU\
  Opens key:                HKCU\software\microsoft\.netframework\policy\standards
  Opens key:                HKLM\software\microsoft\.netframework\policy\standards
  Opens key:                HKLM\software\microsoft\.netframework\policy\standards\v2.0.50727
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcr80.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorwks.dll
  Opens key:                HKCU\software\microsoft\.netframework
  Opens key:                HKLM\software\microsoft\fusion
  Opens key:                HKCU\software\microsoft\fusion
  Opens key:
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets
  Opens key:
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\internet
  Opens key:
HKLM\software\microsoft\.netframework\security\policy\extensions\namedpermissionsets\localintranet
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                HKLM\software\microsoft\.netframework\v2.0.50727\security\policy
  Opens key:                HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32
  Opens key:                HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\mscorlib.ni.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\0fe92a59448dcd7b0d7f239c237a351e.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\77\20f75277
  Opens key:                HKLM\software\microsoft\net framework setup\dotnetclient\v3.5
  Opens key:                HKLM\software\microsoft\strongname
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorjit.dll
  Opens key:                HKLM\software\microsoft\fusion\publisherpolicy\default
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\340b8570\4f
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7
  Opens key:                HKLM\software\microsoft\.netframework\policy\aptca
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17
  Opens key:                HKCU\software\5cd8f17f4086744065eb0992a09e05a2
  Opens key:                HKCU\environment
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.ni.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\microsoft.visualbasic.ni.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.drawing.ni.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.windows.forms.ni.dll
  Opens key:                HKLM\software\microsoft\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\0fe92a59448dcd7b0d7f239c237a351e.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\0fe92a59448dcd7b0d7f239c237a351e.exe
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
  Opens key:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
  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:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\fileexts\.exe
  Opens key:                HKCU\software\classes\.exe
  Opens key:                HKCR\.exe
  Opens key:                HKCU\software\classes\exefile
  Opens key:                HKCR\exefile
  Opens key:                HKCU\software\classes\exefile\curver
  Opens key:                HKCR\exefile\curver
  Opens key:                HKCR\exefile\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\system
  Opens key:                HKCU\software\classes\exefile\shellex\iconhandler
  Opens key:                HKCR\exefile\shellex\iconhandler
  Opens key:                HKCU\software\classes\systemfileassociations\.exe
  Opens key:                HKCR\systemfileassociations\.exe
  Opens key:                HKCU\software\classes\systemfileassociations\application
  Opens key:                HKCR\systemfileassociations\application
  Opens key:                HKCU\software\classes\exefile\clsid
  Opens key:                HKCR\exefile\clsid
  Opens key:                HKCU\software\classes\*
  Opens key:                HKCR\*
  Opens key:                HKCU\software\classes\*\clsid
  Opens key:                HKCR\*\clsid
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:                HKLM\system\currentcontrolset\control\minint
  Opens key:                HKLM\system\wpa\pnp
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key:                HKLM\software\policies\microsoft\system\dnsclient
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}\
  Opens key:                HKCU\software\classes\directory
  Opens key:                HKCR\directory
  Opens key:                HKCU\software\classes\directory\curver
  Opens key:                HKCR\directory\curver
  Opens key:                HKCR\directory\
  Opens key:                HKCU\software\classes\directory\shellex\iconhandler
  Opens key:                HKCR\directory\shellex\iconhandler
  Opens key:                HKCU\software\classes\directory\clsid
  Opens key:                HKCR\directory\clsid
  Opens key:                HKCU\software\classes\folder
  Opens key:                HKCR\folder
  Opens key:                HKCU\software\classes\folder\clsid
  Opens key:                HKCR\folder\clsid
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shellexecutehooks
  Opens key:                HKCU\software\classes\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32
  Opens key:                HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\associations
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\associations
  Opens key:                HKCU\software\classes\.ade
  Opens key:                HKCR\.ade
  Opens key:                HKCU\software\classes\.adp
  Opens key:                HKCR\.adp
  Opens key:                HKCU\software\classes\.app
  Opens key:                HKCR\.app
  Opens key:                HKCU\software\classes\.asp
  Opens key:                HKCR\.asp
  Opens key:                HKCU\software\classes\.bas
  Opens key:                HKCR\.bas
  Opens key:                HKCU\software\classes\.bat
  Opens key:                HKCR\.bat
  Opens key:                HKCU\software\classes\.cer
  Opens key:                HKCR\.cer
  Opens key:                HKCU\software\classes\.chm
  Opens key:                HKCR\.chm
  Opens key:                HKCU\software\classes\.cmd
  Opens key:                HKCR\.cmd
  Opens key:                HKCU\software\classes\.com
  Opens key:                HKCR\.com
  Opens key:                HKCU\software\classes\.cpl
  Opens key:                HKCR\.cpl
  Opens key:                HKCU\software\classes\.crt
  Opens key:                HKCR\.crt
  Opens key:                HKCU\software\classes\.csh
  Opens key:                HKCR\.csh
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKLM\software\classes
  Opens key:                HKU\
  Opens key:                HKCR\clsid
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\treatas
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\treatas
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserverx86
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver32
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver32
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandler32
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprochandlerx86
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\localserver
  Opens key:                HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\urlmon.dll
  Opens key:                HKCU\software\classes\protocols\name-space handler\
  Opens key:                HKCR\protocols\name-space handler
  Opens key:                HKCU\software\classes\protocols\name-space handler
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\policies\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKLM\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet explorer\main\featurecontrol
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_ignore_policies_zonemap_if_esc_enabled_kb918915
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_unc_savedfilecheck
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_check_zonemap_policy_kb941001
  Opens key:                HKLM\software\policies
  Opens key:                HKCU\software\policies
  Opens key:                HKCU\software
  Opens key:                HKLM\software
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\ranges\
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\zonemap\protocoldefaults\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com
  Opens key:                 HKLM\software\microsoft\windows\currentversion\internet
settings\zonemap\domains\msn.com\related
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_ietldlist_for_domain_determination
  Opens key:                 HKCU\software\microsoft\internet explorer\ietld
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_initialize_urlaction_shellexecute_to_allow_kb936610
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_http_username_password_disable
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_reverse_solidus_in_userinfo_kb932562
  Opens key:                 HKLM\software\policies\microsoft\internet explorer
  Opens key:                 HKLM\software\policies\microsoft\internet explorer\security
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\0
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\1
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\2
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\3
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet settings\zones\4
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\0
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\1
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\zones\2
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\zones\3
  Opens key:                 HKCU\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\4
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\0
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\1
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\2
  Opens key:                 HKCU\software\microsoft\windows\currentversion\internet
```

```
settings\lockdown_zones\3
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\3
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:                HKLM\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:                HKCU\software\policies\microsoft\windows\currentversion\internet
settings\lockdown_zones\4
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_zones_default_drive_intranet_kb941000
  Opens key:                HKCU\software\classes\exefile\shell
  Opens key:                HKCR\exefile\shell
  Opens key:                HKCU\software\classes\exefile\shell\open
  Opens key:                HKCR\exefile\shell\open
  Opens key:                HKCU\software\classes\exefile\shell\open\command
  Opens key:                HKCR\exefile\shell\open\command
  Opens key:
HKCU\software\microsoft\windows\currentversion\policies\explorer\restrictrun
  Opens key:                HKLM\software\microsoft\windows\currentversion\app paths\trojan.exe
  Opens key:                HKCU\software\classes\exefile\shell\open\ddeexec
  Opens key:                HKCR\exefile\shell\open\ddeexec
  Opens key:                HKCU\software\classes\applications\trojan.exe
  Opens key:                HKCR\applications\trojan.exe
  Opens key:                HKCU\software\microsoft\windows\shellnoroam
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:                HKLM\system\wpa\tabletpc
  Opens key:                HKLM\system\wpa\mediacenter
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\trojan.exe
  Opens key:                HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\trojan.exe
  Opens key:                HKLM\software\microsoft\ctf\compatibility\trojan.exe
  Opens key:                HKCU\software\classes\appid\0fe92a59448dcd7b0d7f239c237a351e.exe
  Opens key:                HKCR\appid\0fe92a59448dcd7b0d7f239c237a351e.exe
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\netsh.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netsh.exe
  Opens key:                HKCU\software\microsoft\windows\currentversion\run
  Opens key:                HKLM\software\microsoft\windows\currentversion\run
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shfolder.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\acgenral.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adsldpc.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\atl.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\activeds.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\samlib.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mprapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winmm.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shimeng.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msacm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
```

```
  Opens key:                HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:                HKLM\system\currentcontrolset\services\netbt\parameters
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1
  Opens key:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2
  Opens key:                HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm
  Opens key:                HKLM\system\currentcontrolset\control\mediaresources\acm
  Opens key:                HKLM\system\currentcontrolset\control\productoptions
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:                HKLM\software\microsoft\netsh
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ipv6mon.dll
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  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\software\microsoft\windows nt\currentversion\image file execution
options\ipmontr.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\trojan.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clusapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:                HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netcfgx.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\credui.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\dot3api.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winsta.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll
  Opens key:              HKLM\system\currentcontrolset\services\crypt32\performance
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcp60.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\eappcfg.dll
  Opens key:              HKLM\system\currentcontrolset\control\wmi\security
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\eappprxy.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\onex.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dot3dlg.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netshell.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ifmon.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ippromon.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasmontr.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ipxmontr.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ipxpromn.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\framedyn.dll
  Opens key:              HKLM\software\microsoft\wbem\cimom
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dgnet.dll
  Opens key:              HKLM\software\microsoft\ctf\compatibility\netsh.exe
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\treatas
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\treatas
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserverx86
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserverx86
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\localserver32
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver32
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandler32
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprochandlerx86
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandlerx86
  Opens key:              HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\localserver
  Opens key:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\localserver
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemcomn.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemprox.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetmon.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fwcfg.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\qutil.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\napmontr.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dot3cfg.dll
  Opens key:              HKLM\software\microsoft\tracing\fwcfg
  Opens key:              HKLM\software\microsoft\cryptography\defaults\provider
  Opens key:              HKLM\software\microsoft\cryptography\defaults\provider\gemplus gemsafe
card csp v1.0
  Opens key:              HKLM\software\microsoft\cryptography\defaults\provider\infineon sicrypt
base smart card csp
  Opens key:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
cryptographic provider v1.0
```

```
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
dss and diffie-hellman cryptographic provider
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
dss cryptographic provider
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft dh
schannel cryptographic provider
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced cryptographic provider v1.0
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced dss and diffie-hellman cryptographic provider
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider (prototype)
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
schannel cryptographic provider
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\schlumberger
cryptographic service provider
  Opens key:                HKLM\software\microsoft\cryptography\oid
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype 0
  Opens key:                HKLM\software\microsoft\cryptography\oid\encodingtype
0\cryptdllfindoidinfo
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\treatas
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\treatas
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprocserver32
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprocserverx86
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\localserver32
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\localserver32
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprochandler32
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprochandlerx86
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\localserver
  Opens key:                HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\qagent.dll
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netsh.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\
  Opens key:
HKLM\system\currentcontrolset\services\napagent\localconfig\enroll\hcsgroups\
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\treatas
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\treatas
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprocserver32
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprocserverx86
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\localserver32
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\localserver32
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprochandler32
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprochandlerx86
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\localserver
  Opens key:                HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\localserver
  Opens key:                HKLM\system\currentcontrolset\services\napagent\qecs\79617
  Opens key:                HKLM\system\currentcontrolset\services\napagent\qecs\79618
  Opens key:                HKLM\system\currentcontrolset\services\napagent\qecs\79619
  Opens key:                HKLM\system\currentcontrolset\services\napagent\qecs\79620
  Opens key:                HKLM\system\currentcontrolset\services\napagent\qecs\79621
  Opens key:                HKLM\system\currentcontrolset\services\napagent\qecs\79623
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79617
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79618
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79619
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79620
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79621
  Opens key:                HKLM\system\currentcontrolset\services\napagent\localconfig\qecs\79623
  Opens key:                HKCU\software\classes\appid\netsh.exe
  Opens key:                HKCR\appid\netsh.exe
  Opens key:                HKLM\software\microsoft\hcs
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\treatas
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserver32
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprocserverx86
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\localserver32
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver32
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandler32
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\inprochandlerx86
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-
00c04fb68820}\localserver
  Opens key:                HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\localserver
  Opens key:                HKCU\software\classes\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
  Opens key:                HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
  Opens key:                HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}
  Opens key:                HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-
00c04fb68820}\proxystubclsid32
  Opens key:                HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\treatas
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\treatas
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserverx86
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\localserver32
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver32
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandler32
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprochandlerx86
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\localserver
  Opens key:                HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wbemsvc.dll
  Opens key:                HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
  Opens key:                HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}
  Opens key:                HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-
930efe48a887}\proxystubclsid32
  Opens key:                HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
  Opens key:                HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}
  Opens key:                HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-
00aa003240c7}\proxystubclsid32
  Opens key:                HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\treatas
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserverx86
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\localserver32
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver32
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandler32
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprochandlerx86
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\localserver
  Opens key:                HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdsapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\fastprox.dll
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12
  Opens key:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d
  Opens key:                HKCU\software\classes\interface\{027947e1-d731-11ce-a357-000000000001}
  Opens key:                HKCR\interface\{027947e1-d731-11ce-a357-000000000001}
  Opens key:                HKCU\software\classes\interface\{027947e1-d731-11ce-a357-
000000000001}\proxystubclsid32
  Opens key:                HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\treatas
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\treatas
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserverx86
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\localserver32
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver32
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandler32
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprochandlerx86
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\localserver
  Opens key:                HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\localserver
  Opens key:                HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
  Opens key:                HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}
  Opens key:                HKCU\software\classes\interface\{1c1c45ee-4395-11d2-b60b-
00104b703efd}\proxystubclsid32
  Opens key:                HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
  Opens key:                HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}
  Opens key:                HKCU\software\classes\interface\{423ec01e-2e35-11d2-b604-
00104b703efd}\proxystubclsid32
  Opens key:                HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.configuration.ni.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.xml.ni.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:                HKLM\system\currentcontrolset\services\.net clr networking\performance
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\treatas
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\treatas
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserverx86
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\localserver32
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\localserver32
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprochandler32
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprochandlerx86
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\localserver
```

```
  Opens key:                HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\localserver
  Opens key:
HKLM\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\treatas
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\treatas
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\inprocserver32
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\inprocserverx86
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\localserver32
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\localserver32
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\inprochandler32
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\inprochandlerx86
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprochandlerx86
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:                HKCU\software\classes\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\localserver
  Opens key:                HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscoree.dll[checkapphelp]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
  Queries value:            HKLM\software\microsoft\.netframework[installroot]
  Queries value:            HKLM\software\microsoft\.netframework[clrloadlogdir]
  Queries value:            HKLM\software\microsoft\.netframework[onlyuselatestclr]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[0fe92a59448dcd7b0d7f239c237a351e]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[0fe92a59448dcd7b0d7f239c237a351e]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mscorwks.dll[checkapphelp]
  Queries value:            HKLM\software\microsoft\.netframework[gcstressstart]
  Queries value:            HKLM\software\microsoft\.netframework[gcstressstartatjit]
  Queries value:            HKLM\software\microsoft\.netframework[disableconfigcache]
  Queries value:            HKLM\software\microsoft\fusion[cachelocation]
  Queries value:            HKLM\software\microsoft\fusion[downloadcachequotainkb]
  Queries value:            HKLM\software\microsoft\fusion[enablelog]
  Queries value:            HKLM\software\microsoft\fusion[logginglevel]
  Queries value:            HKLM\software\microsoft\fusion[forcelog]
  Queries value:            HKLM\software\microsoft\fusion[logfailures]
  Queries value:            HKLM\software\microsoft\fusion[versioninglog]
  Queries value:            HKLM\software\microsoft\fusion[logresourcebinds]
  Queries value:            HKLM\software\microsoft\fusion[uselegacyidentityformat]
  Queries value:            HKLM\software\microsoft\fusion[disablemsipeek]
  Queries value:            HKLM\software\microsoft\fusion[noclientchecks]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  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\user shell
folders[appdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32[latestindex]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c[niusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\index9c[ilusagemask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configmask]
```

```
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\181938c6\7950e2c5\8[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\7950e2c5\3838a3a4\8[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[mscorlib,2.0.0.0,,b77a5c561934e089,x86]
   Queries value:             HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
   Queries value:             HKLM\software\microsoft\ole[rwlockresourcetimeout]
   Queries value:             HKCR\interface[interfacehelperdisableall]
   Queries value:             HKCR\interface[interfacehelperdisableallforole32]
   Queries value:             HKCR\interface[interfacehelperdisabletypelib]
   Queries value:             HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
   Queries value:             HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
   Queries value:             HKLM\software\microsoft\ctf\systemshared[cuas]
   Queries value:             HKCU\keyboard layout\toggle[language hotkey]
   Queries value:             HKCU\keyboard layout\toggle[hotkey]
   Queries value:             HKCU\keyboard layout\toggle[layout hotkey]
   Queries value:             HKLM\software\microsoft\ctf[enableanchorcontext]
   Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
   Queries value:             HKLM\software\microsoft\fusion\publisherpolicy\default[latest]
   Queries value:             HKLM\software\microsoft\fusion\publisherpolicy\default[index1]
   Queries value:
HKLM\software\microsoft\fusion\publisherpolicy\default[legacypolicytimestamp]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\1c22df2f\4f99a7c9\3f[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\c991064\3880e29a\1d[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\6dc7d4c0\7cd935b4\e[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[displayname]
   Queries value:
```

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3ced59c5\32e43dd1\d[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\f6e8397\9edd04c\4e[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2b1a4e4\502472a2\3e[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\24bf93f6\129642c9\22[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\340b8570\4f[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\340b8570\4f[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\340b8570\4f[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\340b8570\4f[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\4f99a7c9\340b8570\4f[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\30bc7c4f\3f50fe4f\7[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\424bd4d8\2bfe65de\5[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\19ab8d57\61dc497f\6[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[displayname]
   Queries value:
```

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\3f50fe4f\7540f5be\7[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[microsoft.visualbasic,8.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system,2.0.0.0,,b77a5c561934e089,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.xml,2.0.0.0,,b77a5c561934e089,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.configuration,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.web,2.0.0.0,,b03f5f7f11d50a3a,x86]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.management,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.remoting,2.0.0.0,,b77a5c561934e089,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.deployment,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.drawing,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.windows.forms,2.0.0.0,,b77a5c561934e089,msil]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\61e7e666\c991064\13[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\475dce40\3856a4e\10[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\2dd6ac50\11bd3c34\30[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[modules]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[sig]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\41c04c7e\286a445d\24[lastmodtime]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[status]
  Queries value:
```

```
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\3cca06a0\6dc7d4c0\17[missingdependencies]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.runtime.serialization.formatters.soap,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[accessibility,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.security,2.0.0.0,,b03f5f7f11d50a3a,msil]
  Queries value:             HKCU\software\5cd8f17f4086744065eb0992a09e05a2[us]
  Queries value:             HKCU\environment[see_mask_nozonechecks]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer[maximizeapps]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer[maximizeapps]
  Queries value:             HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Queries value:             HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
  Queries value:             HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[allowfileclsidjunctions]
  Queries value:             HKCR\.exe[]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Queries value:             HKCR\exefile[docobject]
  Queries value:             HKCR\exefile[browseinplace]
  Queries value:             HKCR\exefile[isshortcut]
  Queries value:             HKCR\exefile[alwaysshowext]
  Queries value:             HKCR\exefile[nevershowext]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:             HKLM\system\wpa\pnp[seed]
  Queries value:             HKLM\system\setup[osloaderpath]
  Queries value:             HKLM\system\setup[systempartition]
  Queries value:             HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
```

```
  Queries value:
HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion[devicepath]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[loglevel]
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[logpath]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
  Queries value:            HKCR\directory[docobject]
  Queries value:            HKCR\directory[browseinplace]
  Queries value:            HKCR\directory[isshortcut]
  Queries value:            HKCR\directory[alwaysshowext]
  Queries value:            HKCR\directory[nevershowext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
  Queries value:            HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value:            HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
  Queries value:            HKCR\clsid\{aeb6717e-7e19-11d0-97ee-00c04fd91972}\inprocserver32[]
  Queries value:            HKCR\clsid\{aeb6717e-7e19-11d0-97ee-
00c04fd91972}\inprocserver32[loadwithoutcom]
  Queries value:            HKCR\.asp[]
  Queries value:            HKCR\.bat[]
  Queries value:            HKCR\.cer[]
  Queries value:            HKCR\.chm[]
  Queries value:            HKCR\.cmd[]
  Queries value:            HKCR\.com[]
  Queries value:            HKCR\.cpl[]
  Queries value:            HKCR\.crt[]
  Queries value:            HKLM\software\microsoft\com3[com+enabled]
  Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateprocess]
  Queries value:            HKLM\software\microsoft\ole[minimumfreemempercentagetocreateobject]
  Queries value:            HKLM\software\microsoft\com3[regdbversion]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}\inprocserver32[]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-00c04fb6bfc4}[appid]
  Queries value:            HKCR\clsid\{7b8a2d94-0ac9-11d1-896c-
00c04fb6bfc4}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[0fe92a59448dcd7b0d7f239c237a351e.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:            HKCU\software\microsoft\internet explorer\ietld[ietlddllversionlow]
  Queries value:            HKCU\software\microsoft\internet explorer\ietld[ietlddllversionhigh]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[createuricachesize]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[enablepunycode]
  Queries value:            HKLM\software\policies\microsoft\internet
explorer\security[disablesecuritysettingscheck]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\1[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\2[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\3[flags]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\4[flags]
  Queries value:            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[0fe92a59448dcd7b0d7f239c237a351e.exe]
  Queries value:            HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[0fe92a59448dcd7b0d7f239c237a351e.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_localmachine_lockdown[*]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[specialfolderscachesize]
```

```
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\zones\0[1806]
  Queries value:            HKCR\exefile\shell[]
  Queries value:            HKCR\exefile\shell\open\command[]
  Queries value:            HKCR\exefile\shell\open\command[command]
  Queries value:            HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
  Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\trojan.exe]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[inheritconsolehandles]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[disallowrun]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[norunasinstallprompt]
  Queries value:            HKLM\system\wpa\mediacenter[installed]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
  Queries value:            HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[itemsize]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemdata]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[hashalg]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[itemsize]
  Queries value:
```

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}[saferflags]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
  Queries value:          HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[trojan]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[trojan]
  Queries value:          HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:          HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:          HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:          HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  Queries value:
HKCU\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
  Queries value:
HKLM\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
  Queries value:          HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[startup]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\compatibility32[netsh]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[netsh]
  Queries value:          HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Queries value:          HKCU\software\microsoft\multimedia\audio[systemformats]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.imaadpcm]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[fdwsupport]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cformattags]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[aformattagcache]
  Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.imaadpcm[cfiltertags]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msadpcm]
```

```
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msadpcm[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg711]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg711[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msgsm610]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msgsm610[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.trspch]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.trspch[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msg723]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msg723[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.msaudio1]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.msaudio1[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows
nt\currentversion\drivers32[msacm.sl_anet]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.sl_anet[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.iac2]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.iac2[cfiltertags]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\drivers32[msacm.l3acm]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[fdwsupport]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cformattags]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[aformattagcache]
   Queries value:
HKLM\software\microsoft\audiocompressionmanager\drivercache\msacm.l3acm[cfiltertags]
   Queries value:              HKCU\software\microsoft\multimedia\audio compression
manager\msacm[nopcmconverter]
```

```
  Queries value:             HKCU\software\microsoft\multimedia\audio compression manager\priority
v4.00[priority1]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:             HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:             HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:             HKCU\control panel\desktop[lamebuttontext]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\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\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\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[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
  Queries value:           HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
  Queries value:
```

```
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion[currentbuildnumber]
  Queries value:              HKLM\software\microsoft\wbem\cimom[logging]
  Queries value:              HKLM\software\microsoft\wbem\cimom[logging directory]
  Queries value:              HKLM\software\microsoft\wbem\cimom[log file max size]
  Queries value:              HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]
  Queries value:              HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[appid]
  Queries value:              HKCR\clsid\{4590f811-1d3a-11d0-891f-
00aa004b2e24}\inprocserver32[threadingmodel]
  Queries value:              HKLM\software\microsoft\wbem\cimom[repository directory]
  Queries value:              HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\fwcfg[enablefiletracing]
  Queries value:              HKLM\software\microsoft\tracing\fwcfg[filetracingmask]
  Queries value:              HKLM\software\microsoft\tracing\fwcfg[enableconsoletracing]
  Queries value:              HKLM\software\microsoft\tracing\fwcfg[consoletracingmask]
  Queries value:              HKLM\software\microsoft\tracing\fwcfg[maxfilesize]
  Queries value:              HKLM\software\microsoft\tracing\fwcfg[filedirectory]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\gemplus gemsafe
card csp v1.0[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\infineon sicrypt
base smart card csp[type]
  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
dss and diffie-hellman cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft base
dss cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft dh
schannel cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced cryptographic provider v1.0[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced dss and diffie-hellman cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft
enhanced rsa and aes cryptographic provider (prototype)[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft rsa
schannel cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\schlumberger
cryptographic service provider[type]
  Queries value:              HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprocserver32[inprocserver32]
  Queries value:              HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}\inprocserver32[]
  Queries value:              HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-28ecbd96ba8c}[appid]
  Queries value:              HKCR\clsid\{ea4a0a43-1c8f-4c7b-a4b1-
28ecbd96ba8c}\inprocserver32[threadingmodel]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[displayname]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[configmask]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[configstring]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[mvid]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[evalationdata]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[status]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[ildependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[nidependencies]
  Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\159a66b8\424bd4d8\2a[missingdependencies]
  Queries value:              HKLM\system\currentcontrolset\services\napagent\localconfig[enable
tracing]
  Queries value:              HKLM\system\currentcontrolset\services\napagent\localconfig[tracing
level]
  Queries value:              HKCR\clsid\{eb082ba1-df8a-46be-82f3-
```

```
35bf9e9be52f}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}\inprocserver32[]
  Queries value:            HKCR\clsid\{eb082ba1-df8a-46be-82f3-35bf9e9be52f}[appid]
  Queries value:            HKCR\clsid\{eb082ba1-df8a-46be-82f3-
35bf9e9be52f}\inprocserver32[threadingmodel]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[friendly
name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[description]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[version]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[enabled]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[vendor name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[info clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[config clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[validator
clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[registration
date]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79617[component
type]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[friendly
name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[description]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[version]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[enabled]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[vendor name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[info clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[config clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[validator
clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[registration
date]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79618[component
type]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[friendly
name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[description]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[version]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[enabled]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[vendor name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[info clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[config clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[validator
clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[registration
date]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79619[component
type]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[friendly
name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[description]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[version]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[enabled]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[vendor name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[info clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[config clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[validator
clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[registration
date]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79620[component
type]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[friendly
name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[description]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[version]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[enabled]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[vendor name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[info clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[config clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[validator
clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[registration
date]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79621[component
type]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[friendly
name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[description]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[version]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[enabled]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[vendor name]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[info clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[config clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[validator
clsid]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[registration
date]
  Queries value:            HKLM\system\currentcontrolset\services\napagent\qecs\79623[component
```

```
type]
   Queries value:
HKLM\system\currentcontrolset\services\napagent\localconfig[plumbipsecpolicy]
   Queries value:              HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[appid]
   Queries value:              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[dllsurrogate]
   Queries value:              HKCR\appid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[localservice]
   Queries value:              HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}\proxystubclsid32[]
   Queries value:              HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]
   Queries value:              HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[appid]
   Queries value:              HKCR\clsid\{7c857801-7381-11cf-884d-
00aa004b2e24}\inprocserver32[threadingmodel]
   Queries value:              HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[]
   Queries value:              HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]
   Queries value:              HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]
   Queries value:              HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[appid]
   Queries value:              HKCR\clsid\{d68af00a-29cb-43fa-8504-
ce99a996d9ea}\inprocserver32[threadingmodel]
   Queries value:              HKLM\software\microsoft\wbem\cimom[processid]
   Queries value:              HKLM\software\microsoft\wbem\cimom[enableprivateobjectheap]
   Queries value:              HKLM\software\microsoft\wbem\cimom[contextlimit]
   Queries value:              HKLM\software\microsoft\wbem\cimom[objectlimit]
   Queries value:              HKLM\software\microsoft\wbem\cimom[identifierlimit]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[configmask]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[configstring]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[mvid]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[evalationdata]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[ildependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[nidependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\ni\6faf58\19ab8d57\12[missingdependencies]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[displayname]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[status]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[modules]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[sig]
   Queries value:
HKLM\software\microsoft\fusion\nativeimagesindex\v2.0.50727_32\il\75638fee\78136415\2d[lastmodtime]
   Queries value:
HKLM\software\microsoft\fusion\gacchangenotification\default[system.data.sqlxml,2.0.0.0,,b77a5c561934e089,msil]
   Queries value:              HKCR\interface\{027947e1-d731-11ce-a357-000000000001}\proxystubclsid32[]
   Queries value:              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}\inprocserver32[]
   Queries value:              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-00104b703efd}[appid]
   Queries value:              HKCR\clsid\{1b1cad8c-2dab-11d2-b604-
00104b703efd}\inprocserver32[threadingmodel]
   Queries value:              HKCR\interface\{1c1c45ee-4395-11d2-b60b-00104b703efd}\proxystubclsid32[]
   Queries value:              HKCR\interface\{423ec01e-2e35-11d2-b604-00104b703efd}\proxystubclsid32[]
   Queries value:              HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
   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\tcpip\parameters\winsock[minsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
   Queries value:              HKLM\system\currentcontrolset\services\.net clr
networking\performance[library]
   Queries value:              HKLM\system\currentcontrolset\services\.net clr
networking\performance[ismultiinstance]
   Queries value:              HKLM\system\currentcontrolset\services\.net clr
networking\performance[first counter]
   Queries value:              HKLM\system\currentcontrolset\services\.net clr
networking\performance[categoryoptions]
   Queries value:              HKLM\system\currentcontrolset\services\.net clr
networking\performance[filemappingsize]
   Queries value:              HKLM\system\currentcontrolset\services\.net clr
networking\performance[counter names]
```

```
   Queries value:              HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}\inprocserver32[]
   Queries value:              HKCR\clsid\{304ce942-6e39-40d8-943a-b913c40c9cd4}[appid]
   Queries value:              HKCR\clsid\{304ce942-6e39-40d8-943a-
b913c40c9cd4}\inprocserver32[threadingmodel]
   Queries value:
HKLM\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list[c:\documents
and settings\admin\local settings\temp\trojan.exe]
   Queries value:              HKCR\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\inprocserver32[inprocserver32]
   Queries value:              HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}\inprocserver32[]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
   Queries value:              HKCR\clsid\{ec9846b3-2762-4a6b-a214-6acb603462d2}[appid]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
   Queries value:              HKCR\clsid\{ec9846b3-2762-4a6b-a214-
6acb603462d2}\inprocserver32[threadingmodel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
   Queries value:              HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
   Queries value:              HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
   Queries value:              HKLM\software\microsoft\cryptography[machineguid]
   Queries value:              HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
   Sets/Creates value:         HKCU\software\5cd8f17f4086744065eb0992a09e05a2[us]
   Sets/Creates value:         HKCU\environment[see_mask_nozonechecks]
   Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\docume~1\admin\locals~1\temp\trojan.exe]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
   Sets/Creates value:
HKLM\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
   Sets/Creates value:
HKLM\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list[c:\documents
and settings\admin\local settings\temp\trojan.exe]
   Value changes:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
   Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
   Value changes:              HKCU\software\microsoft\windows\currentversion\explorer\shell
```

```
folders[personal]
  Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
  Value changes:            HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common documents]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Value changes:            HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common desktop]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[proxybypass]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[intranetname]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[uncasintranet]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\zonemap[autodetect]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[startup]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[logsessionname]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[active]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg[controlflags]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier[guid]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappcfg\traceidentifier[bitnames]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[logsessionname]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[active]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy[controlflags]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy\traceidentifier[guid]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\eappprxy\traceidentifier[bitnames]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[logsessionname]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[active]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil[controlflags]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil\traceidentifier[guid]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qutil\traceidentifier[bitnames]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh[logsessionname]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh[active]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh[controlflags]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh\napmontr[guid]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\nap\netsh\napmontr[bitnames]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent[logsessionname]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent[active]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent[controlflags]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent\traceidentifier[guid]
  Value changes:            HKLM\software\microsoft\windows
nt\currentversion\tracing\microsoft\qagent\traceidentifier[bitnames]
  Value changes:
HKCU\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
  Value changes:
HKLM\software\microsoft\windows\currentversion\run[5cd8f17f4086744065eb0992a09e05a2]
```