Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	744
Risk Level:	10
Date Processed:	2016-05-18 10:33:01 (UTC)
Processing Time:	61.58 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe"
Sample ID:	3309
Type:	basic
Owner:	admin
Label:	6b0dfa86acf4bfbdf5c34927f9b3e733
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	155648 bytes
MD5:	6b0dfa86acf4bfbdf5c34927f9b3e733
SHA256:	2a5e99090310812a6d7d02c07e70d3fc29d3588998de27d4f54e4a5f73a017f3
Description:	None

Pattern Matching Results

6 Modifies registry autorun entries
10 Creates malicious events: Vobfus [Worm]
5 Adds autostart object
5 Creates process in suspicious location

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe ["c:\windows\temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe"]
Creates process:	C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe [71]
Creates process:	C:\Documents and Settings\Admin\boauh.exe ["C:\Documents and Settings\Admin\boauh.exe"]
Creates process:	C:\Documents and Settings\Admin\boauh.exe [71]
Writes to process:	PID:1884 C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe
Writes to process:	PID:504 C:\Documents and Settings\Admin\boauh.exe
Terminates process:	C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe
Terminates process:	C:\Documents and Settings\Admin\boauh.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\A
Creates mutex:	\BaseNamedObjects\ZonesCounterMutex
Creates mutex:	\BaseNamedObjects\ZoneAttributeCacheCounterMutex
Creates mutex:	\BaseNamedObjects\ZonesCacheCounterMutex
Creates mutex:	\BaseNamedObjects\ZonesLockedCacheCounterMutex
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\C:?WINDOWS?TEMP?6B0DFA86ACF4BFBDF5C34927F9B3E733.EXE
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}
Creates semaphore:	\BaseNamedObjects\C:?DOCUMENTS AND SETTINGS?ADMIN?BOAUH.EXE

File System Events

Creates:	C:\Documents and Settings\Admin\boauh.exe
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\msvbvm60.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\sxs.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\Registration\R000000000007.clb
Opens:	C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe
Opens:	C:\WINDOWS\system32\apphelp.dll

```
Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
Opens:                  C:\WINDOWS\AppPatch\systest.sdb
Opens:                  C:\WINDOWS\Temp
Opens:                  C:\
Opens:                  C:\WINDOWS
Opens:                  C:\windows\temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe.Manifest
Opens:                  C:\WINDOWS\Prefetch\6B0DFA86ACF4BFBDF5C34927F9B3E-0FAA7DB6.pf
Opens:                  C:\WINDOWS\WINHELP.INI
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\boauh.exe
Opens:                  C:\WINDOWS\system32\netapi32.dll
Opens:                  C:\WINDOWS\system32\setupapi.dll
Opens:                  C:\Documents and Settings
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\urlmon.dll
Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Manifest
Opens:                  C:\WINDOWS\system32\urlmon.dll.123.Config
Opens:                  C:\Documents and Settings\Admin\boauh.exe.Manifest
Opens:                  C:\WINDOWS\Prefetch\BOAUH.EXE-053BB084.pf
Opens:                  C:\WINDOWS\system32\ws2_32.dll
Opens:                  C:\WINDOWS\system32\ws2help.dll
Opens:                  C:\WINDOWS\system32\mswsock.dll
Opens:                  C:\WINDOWS\system32\hnetcfg.dll
Opens:                  C:\WINDOWS\system32\wshtcpip.dll
Opens:                  C:\WINDOWS\system32\dnsapi.dll
Opens:                  C:\WINDOWS\system32\iphlpapi.dll
Opens:                  C:\WINDOWS\system32\winrnr.dll
Opens:                  C:\WINDOWS\system32\drivers\etc\hosts
Opens:                  C:\WINDOWS\system32\rsaenh.dll
Opens:                  C:\WINDOWS\system32\crypt32.dll
Opens:                  C:\WINDOWS\system32\rasadhlp.dll
Opens:                  C:\WINDOWS\system32\MSIMTF.dll
Writes to:              C:\Documents and Settings\Admin\boauh.exe
Reads from:             C:\WINDOWS\Registration\R000000000007.clb
Reads from:             C:\WINDOWS\Temp\6b0dfa86acf4bfbdf5c34927f9b3e733.exe
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:\Documents and Settings\Admin\boauh.exe
Reads from:             C:\WINDOWS\system32\drivers\etc\hosts
Reads from:             C:\WINDOWS\system32\rsaenh.dll
```

Network Events

```
DNS query:         ns1.boxonline1.com
DNS query:         ns1.boxonline1.net
DNS query:         ns1.boxonline1.org
DNS query:         ns1.boxonline2.com
DNS query:         ns1.boxonline2.net
DNS query:         ns1.boxonline2.org
DNS query:         ns1.boxonline3.com
DNS query:         ns1.boxonline3.net
DNS query:         ns1.boxonline3.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:
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\windows\currentversion\run\
Creates key:       HKCU\software\Pre\microsoft\windows\currentversion\explorer\advanced\
Creates key:       HKLM\software\policies\microsoft\windows\windowsupdate\au
Creates key:       HKLM\software
Creates key:       HKLM\software\policies
```

```
 Creates key:              HKLM\software\policies\microsoft
 Creates key:              HKLM\software\policies\microsoft\windows
 Creates key:              HKLM\software\policies\microsoft\windows\windowsupdate
 Creates key:              HKLM\system\currentcontrolset\services\tcpip\parameters
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6b0dfa86acf4bfbdf5c34927f9b3e733.exe
 Opens key:                HKLM\system\currentcontrolset\control\terminal server
 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\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
 Opens key:                HKLM\system\currentcontrolset\control\session manager
 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\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\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\image file execution
options\msvcrt.dll
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvbvm60.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 nt\currentversion\winlogon
 Opens key:                HKLM\
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
 Opens key:                HKLM\software\microsoft\ole
 Opens key:                HKCR\interface
 Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
 Opens key:                HKLM\software\microsoft\oleaut
 Opens key:                HKLM\software\microsoft\oleaut\userera
 Opens key:                HKCU\
 Opens key:                HKCU\software\policies\microsoft\control panel\desktop
 Opens key:                HKCU\control panel\desktop
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
 Opens key:
HKLM\software\microsoft\ctf\compatibility\6b0dfa86acf4bfbdf5c34927f9b3e733.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\windows nt\currentversion\image file execution
options\sxs.dll
 Opens key:                HKLM\system\setup
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
 Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
 Opens key:                HKCU\software\microsoft\ctf
 Opens key:                HKLM\software\microsoft\ctf\systemshared
 Opens key:                HKLM\system\currentcontrolset\control\nls\codepage
 Opens key:                HKLM\software\microsoft\vba\monitors
 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\clbcatq.dll
 Opens key:                HKLM\software\microsoft\com3\debug
 Opens key:                HKCU\software\classes\
 Opens key:                HKLM\software\classes
 Opens key:                HKU\
 Opens key:                HKCR\clsid
 Opens key:                HKCU\software\classes\clsid\{a4341dcc-5064-42df-9638-3b4a33c14bd4}
```

```
Opens key:                HKCR\clsid\{a4341dcc-5064-42df-9638-3b4a33c14bd4}
Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
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\6b0dfa86acf4bfbdf5c34927f9b3e733.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
   Opens key:              HKLM\software\microsoft\windows\html help
   Opens key:              HKLM\software\microsoft\windows\help
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
   Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\performance
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
   Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
   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\windows nt\currentversion\image file execution
options\userenv.dll
   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:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
   Opens key:              HKLM\system\currentcontrolset\services\disk\enum
   Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\6b0dfa86acf4bfbdf5c34927f9b3e733.exe
   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\rpc\pagedbuffers
   Opens key:              HKLM\software\microsoft\rpc
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6b0dfa86acf4bfbdf5c34927f9b3e733.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\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
   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:              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\boauh.exe
Opens key:              HKCU\software\classes\exefile\shell\open\ddeexec
Opens key:              HKCR\exefile\shell\open\ddeexec
Opens key:              HKCU\software\classes\applications\boauh.exe
Opens key:              HKCR\applications\boauh.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\software\microsoft\windows
nt\currentversion\appcompatflags\custom\boauh.exe
```

```
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\boauh.exe
  Opens key:               HKLM\software\microsoft\ctf\compatibility\boauh.exe
  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\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\mswsock.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\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.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\iphlpapi.dll
  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\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
  Opens key:               HKLM\system\currentcontrolset\services\ldap
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
  Opens key:               HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  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\system\currentcontrolset\control\wmi\security
```

```
    Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
    Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
    Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
    Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
    Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[6b0dfa86acf4bfbdf5c34927f9b3e733]
    Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[6b0dfa86acf4bfbdf5c34927f9b3e733]
    Queries value:          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
    Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
    Queries value:          HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
    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:          HKCU\control panel\desktop[multiuilanguageid]
    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:          HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
    Queries value:          HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
    Queries value:          HKCU\software\microsoft\ctf[disable thread input manager]
    Queries value:          HKLM\system\currentcontrolset\control\nls\codepage[932]
    Queries value:          HKLM\system\currentcontrolset\control\nls\codepage[949]
    Queries value:          HKLM\system\currentcontrolset\control\nls\codepage[950]
    Queries value:          HKLM\system\currentcontrolset\control\nls\codepage[936]
    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:          HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
    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\system\setup[systemsetupinprogress]
   Queries value: HKCU\control panel\desktop[smoothscroll]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
   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[personal]
   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: HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-1757981266-507921405-1957994488-1003[profileimagepath]
   Queries value: HKLM\system\currentcontrolset\services\disk\enum[0]
   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:              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:
HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
   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:              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[6b0dfa86acf4bfbdf5c34927f9b3e733.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[6b0dfa86acf4bfbdf5c34927f9b3e733.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[6b0dfa86acf4bfbdf5c34927f9b3e733.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[cache]
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:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[userpreference]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[centralprofile]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimelow]
Queries value:              HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimehigh]
Queries value:              HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
Queries value:              HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and
settings\admin\boauh.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\software\microsoft\windows nt\currentversion\compatibility32[boauh]
   Queries value:              HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[boauh]
   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\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\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\services\tcpip\linkage[bind]
    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:
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\system\currentcontrolset\services\ldap[ldapclientintegrity]
    Queries value:           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
    Queries value:           HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
```

```
Queries value:              HKLM\software\microsoft\cryptography[machineguid]
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\system\currentcontrolset\services\winsock2\parameters[autodialdll]
Queries value:              HKLM\software\microsoft\windows\currentversion[programfilesdir]
Sets/Creates value:         HKCU\software\microsoft\windows\shellnoroam\muicache[c:\documents and
settings\admin\boauh.exe]
Sets/Creates value:         HKCU\software\microsoft\windows\currentversion\run[boauh]
Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Sets/Creates value:         HKLM\software\policies\microsoft\windows\windowsupdate\au[noautoupdate]
Value changes:              HKLM\software\microsoft\cryptography\rng[seed]
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[cache]
Value changes:              HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
Value changes:              HKCU\software\microsoft\windows\currentversion\run[boauh]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
Value changes:              HKLM\software\policies\microsoft\windows\windowsupdate\au[noautoupdate]
```