Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	515
Risk Level:	6
Date Processed:	2016-04-28 13:01:20 (UTC)
Processing Time:	3.35 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\adb62392bc0711707e58e70186cc4ac2.exe"

Sample ID:	129
Type:	basic
Owner:	admin
Label:	adb62392bc0711707e58e70186cc4ac2
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	10224 bytes
MD5:	adb62392bc0711707e58e70186cc4ac2
SHA256:	2d34179da23d345fb5e9d241b34902c188fbf914f3985a7ffb3978dd9ff0287b
Description:	None

Pattern Matching Results

4	Terminates process under Windows subfolder
6	Renames file on boot

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\adb62392bc0711707e58e70186cc4ac2.exe ["c:\windows\temp\adb62392bc0711707e58e70186cc4ac2.exe"]
Creates process:	C:\WINDOWS\system32\schtasks.exe ["C:\WINDOWS\system32\schtasks.exe" /Delete /TN EPUpdater /F]
Terminates process:	C:\WINDOWS\Temp\adb62392bc0711707e58e70186cc4ac2.exe
Terminates process:	C:\WINDOWS\system32\schtasks.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 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

Opens:	C:\WINDOWS\Prefetch\ADB62392BC0711707E58E70186CC4-0C9E3A3E.pf

```
  Opens:                 C:\Documents and Settings\Admin
  Opens:                 C:\WINDOWS\system32\imm32.dll
  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:\WINDOWS\system32\rpcss.dll
  Opens:                 C:\WINDOWS\system32\MSCTF.dll
  Opens:                 C:\WINDOWS\system32\netapi32.dll
  Opens:                 C:\WINDOWS\system32\setupapi.dll
  Opens:                 C:\
  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\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:\WINDOWS
  Opens:                 C:\WINDOWS\system32
  Opens:                 C:\WINDOWS\system32\schtasks.exe
  Opens:                 C:\WINDOWS\system32\apphelp.dll
  Opens:                 C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                 C:\WINDOWS\AppPatch\systest.sdb
  Opens:                 C:\WINDOWS\system32\schtasks.exe.Manifest
  Opens:                 C:\WINDOWS\Temp\adb62392bc0711707e58e70186cc4ac2.exe
  Opens:                 C:\WINDOWS\Prefetch\SCHTASKS.EXE-0CBF6A11.pf
  Opens:                 C:\WINDOWS\system32\ws2_32.dll
  Opens:                 C:\WINDOWS\system32\ws2help.dll
  Opens:                 C:\WINDOWS\system32\shimeng.dll
  Opens:                 C:\WINDOWS\AppPatch\AcGenral.dll
  Opens:                 C:\WINDOWS\system32\winmm.dll
  Opens:                 C:\WINDOWS\system32\msacm32.dll
  Opens:                 C:\WINDOWS\system32\uxtheme.dll
  Opens:                 C:\WINDOWS\system32\winlogon.exe
  Opens:                 C:\WINDOWS\system32\xpsp2res.dll
  Opens:                 C:\WINDOWS\system32\mstask.dll
  Opens:                 C:\WINDOWS\system32\mstask.dll.2.Manifest
  Opens:                 C:\WINDOWS\system32\mstask.dll.2.Config
  Opens:                 C:\WINDOWS\system32\ntdsapi.dll
  Opens:                 C:\WINDOWS\system32\dnsapi.dll
  Opens:                 C:\WINDOWS\Tasks
  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:\WINDOWS\system32\schtasks.exe
```

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:              HKLM\system\currentcontrolset\control\session manager
  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
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\adb62392bc0711707e58e70186cc4ac2.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  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\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  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\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\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\software\microsoft\windows nt\currentversion\image file execution
options\shell32.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:                HKLM\system\setup
  Opens key:                HKCU\
  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\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\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\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\adb62392bc0711707e58e70186cc4ac2.exe
  Opens key:             HKLM\software\microsoft\ctf\systemshared\
  Opens key:             HKCU\keyboard layout\toggle
  Opens key:             HKLM\software\microsoft\ctf\
  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\adb62392bc0711707e58e70186cc4ac2.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\
  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\schtasks.exe
  Opens key:                 HKCU\software\classes\exefile\shell\open\ddeexec
  Opens key:                 HKCR\exefile\shell\open\ddeexec
  Opens key:                 HKCU\software\classes\applications\schtasks.exe
  Opens key:                 HKCR\applications\schtasks.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\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:                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                 HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\schtasks.exe
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\appcompatflags
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\appcompatflags
  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\schtasks.exe
  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\mpr.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\shimeng.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\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\control\networkprovider\hworder
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  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\ctf\compatibility\schtasks.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\schtasks.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\treatas
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\treatas
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprocserver32
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprocserverx86
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\localserver32
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\localserver32
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprochandler32
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprochandlerx86
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\localserver
  Opens key:                HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comdlg32.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\wldap32.dll
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  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\mstask.dll
```

```
 Opens key:                HKLM\software\microsoft\schedulingagent
 Opens key:                HKLM\system\currentcontrolset\control\nls\locale
 Opens key:                HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
 Opens key:                HKLM\system\currentcontrolset\control\nls\language groups
 Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value:            HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value:            HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
 Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[adb62392bc0711707e58e70186cc4ac2]
 Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[adb62392bc0711707e58e70186cc4ac2]
 Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value:            HKLM\system\setup[systemsetupinprogress]
 Queries value:            HKCU\control panel\desktop[multiuilanguageid]
 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\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[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[adb62392bc0711707e58e70186cc4ac2.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[adb62392bc0711707e58e70186cc4ac2.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[adb62392bc0711707e58e70186cc4ac2.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:               HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
  Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\schtasks.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\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\currentcontrolset\control\session
manager[pendingfilerenameoperations2]
  Queries value:              HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
  Queries value:              HKLM\software\microsoft\windows
nt\currentversion\compatibility32[schtasks]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[schtasks]
  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:              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\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:            HKCR\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}\inprocserver32[]
  Queries value:            HKCR\clsid\{148bd52a-a2ab-11ce-b11f-00aa00530503}[appid]
  Queries value:            HKCR\clsid\{148bd52a-a2ab-11ce-b11f-
00aa00530503}\inprocserver32[threadingmodel]
  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\ldap[ldapclientintegrity]
  Queries value:               HKLM\software\microsoft\schedulingagent[tasksfolder]
  Queries value:              HKLM\software\microsoft\schedulingagent[notifyontaskmiss]
  Queries value:              HKLM\software\microsoft\schedulingagent[viewhiddentasks]
  Queries value:              HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:              HKLM\system\currentcontrolset\control\nls\language groups[1]
  Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\schtasks.exe]
  Sets/Creates value:         HKLM\system\currentcontrolset\control\session
manager[pendingfilerenameoperations]
  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[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]
```