Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 3334, Task ID: 844

Task ID:	844
Risk Level:	6
Date Processed:	2016-05-18 10:45:28 (UTC)
Processing Time:	61.22 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\758e49c5f3fae3fd55f5c26204023b81.exe"
Sample ID:	3334
Type:	basic
Owner:	admin
Label:	758e49c5f3fae3fd55f5c26204023b81
Date Added:	2016-05-18 10:30:52 (UTC)
File Type:	PE32:win32:gui
File Size:	344064 bytes
MD5:	758e49c5f3fae3fd55f5c26204023b81
SHA256:	0c71ca797853ba4553280fecadc2c082abd618e793e5bd718a8c6fd780abcc18
Description:	None

Pattern Matching Results

3	Program causes a crash [Info]
2	PE: Nonstandard section
4	Reads process memory
3	Long sleep detected
6	Suspicious packer: VMProtect

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\758e49c5f3fae3fd55f5c26204023b81.exe ["c:\windows\temp\758e49c5f3fae3fd55f5c26204023b81.exe"]
Creates process:	C:\WINDOWS\system32\dwwin.exe [C:\WINDOWS\system32\dwwin.exe -x -s 436]
Loads service:	RASMAN [C:\WINDOWS\system32\svchost.exe -k netsvcs]
Reads from process:	PID:132 C:\WINDOWS\Temp\758e49c5f3fae3fd55f5c26204023b81.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\SHIMLIB_LOG_MUTEX
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local settings!temporary internet files!content.ie5!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!cookies!
Creates mutex:	\BaseNamedObjects\c:!documents and settings!admin!local settings!history!history.ie5!
Creates mutex:	\BaseNamedObjects\WininetConnectionMutex
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates event:	\BaseNamedObjects\{6295DF2D-35EE-11d1-8707-00C04FD93327}CFactEvent_WinSta0_Default
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore:	\BaseNamedObjects\MsoDWExclusive132

File System Events

Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\a0e7_appcompat.txt
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\A56D5F.dmp
Opens:	C:\Documents and Settings\Admin
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\system32\mobsync.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config

```
  Opens:                  C:\WINDOWS\system32\rpcss.dll
  Opens:                  C:\WINDOWS\system32\MSCTF.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\system32\winlogon.exe
  Opens:                  C:\WINDOWS\system32\xpsp2res.dll
  Opens:                  C:\WINDOWS\system32\faultrep.dll
  Opens:                  C:\WINDOWS\system32\winsta.dll
  Opens:                  C:\WINDOWS\system32\netapi32.dll
  Opens:                  C:\WINDOWS\system32\wtsapi32.dll
  Opens:                  C:\WINDOWS\system32\setupapi.dll
  Opens:                  C:\WINDOWS\system32\uxtheme.dll
  Opens:                  C:\
  Opens:                  C:\WINDOWS
  Opens:                  C:\WINDOWS\system32\apphelp.dll
  Opens:                  C:\WINDOWS\Temp\eb6cd1e7-8072-44fb-940b-f6de291c940e
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp
  Opens:                  C:\WINDOWS\Temp
  Opens:                  C:\WINDOWS\Temp\758e49c5f3fae3fd55f5c26204023b81.exe
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\a0e7_appcompat.txt
  Opens:                  C:\WINDOWS\system32
  Opens:                  C:\WINDOWS\system32\kernel32.dll
  Opens:                  C:\WINDOWS\system32\dwwin.exe
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WINDOWS\system32\dwwin.exe.Manifest
  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\comctl32.dll
  Opens:                  C:\WINDOWS\system32\COMCTL32.DLL.124.Manifest
  Opens:                  C:\WINDOWS\system32\COMCTL32.DLL.124.Config
  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\system32\URLMON.DLL.123.Manifest
  Opens:                  C:\WINDOWS\system32\URLMON.DLL.123.Config
  Opens:                  C:\WINDOWS\system32\WININET.DLL.123.Manifest
  Opens:                  C:\WINDOWS\system32\WININET.DLL.123.Config
  Opens:                  C:\WINDOWS\system32\riched20.dll
  Opens:                  C:\WINDOWS\system32\shfolder.dll
  Opens:                  C:\WINDOWS\system32\psapi.dll
  Opens:                  C:\WINDOWS\system32\ntdll.dll
  Opens:                  C:\WINDOWS\system32\msvcrt.dll
  Opens:                  C:\WINDOWS\system32\advapi32.dll
  Opens:                  C:\WINDOWS\system32\rpcrt4.dll
  Opens:                  C:\WINDOWS\system32\secur32.dll
  Opens:                  C:\WINDOWS\system32\gdi32.dll
  Opens:                  C:\WINDOWS\system32\user32.dll
  Opens:                  C:\WINDOWS\system32\ole32.dll
  Opens:                  C:\WINDOWS\system32\shlwapi.dll
  Opens:                  C:\WINDOWS\system32\userenv.dll
  Opens:                  C:\WINDOWS\system32\oleaut32.dll
  Opens:                  C:\WINDOWS\system32\version.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temp\A56D5F.dmp
  Opens:                  C:\WINDOWS\system32\1033\dwintl.dll
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
  Opens:                  C:\Documents and Settings\Admin\Local Settings\History
  Opens:                  C:\Documents and Settings\Admin\Local Settings\History\History.IE5
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
  Opens:                  C:\Documents and Settings\Admin\Cookies
  Opens:                  C:\Documents and Settings\Admin\Cookies\index.dat
  Opens:                  C:\Documents and Settings\Admin\Local
Settings\History\History.IE5\index.dat
  Opens:                  C:\WINDOWS\system32\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\WINDOWS\system32\rasapi32.dll
  Opens:                  C:\WINDOWS\system32\rasman.dll
  Opens:                  C:\WINDOWS\system32\tapi32.dll
  Opens:                  C:\WINDOWS\system32\rtutils.dll
  Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\TAPI32.dll.124.Config
  Opens:                  C:\AUTOEXEC.BAT
  Opens:                  C:\Documents and Settings\All Users\Application
Data\Microsoft\Network\Connections\Pbk
  Opens:                  C:\WINDOWS\system32\ras
  Opens:                  C:\Documents and Settings\Admin\Application
```

```
Data\Microsoft\Network\Connections\Pbk\
  Opens:                    C:\WINDOWS\system32\sensapi.dll
  Opens:                    C:\WINDOWS\Fonts\sserife.fon
  Opens:                    C:\WINDOWS\win.ini
  Opens:                    C:\WINDOWS\system32\msv1_0.dll
  Opens:                    C:\WINDOWS\system32\iphlpapi.dll
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\a0e7_appcompat.txt
  Writes to:                C:\Documents and Settings\Admin\Local Settings\Temp\A56D5F.dmp
  Reads from:               C:\WINDOWS\Registration\R000000000007.clb
  Reads from:               C:\WINDOWS\Temp\758e49c5f3fae3fd55f5c26204023b81.exe
  Reads from:               C:\AUTOEXEC.BAT
  Reads from:               C:\WINDOWS\win.ini
```

Windows Registry Events

```
  Creates key:              HKLM\software\microsoft\windows\currentversion\syncmgr\handlers
  Creates key:              HKLM\software\microsoft\pchealth\errorreporting
  Creates key:              HKLM\software\microsoft\pchealth\errorreporting\exclusionlist
  Creates key:              HKLM\software\microsoft\pchealth\errorreporting\inclusionlist
  Creates key:              HKCU\software\microsoft\windows\currentversion\internet settings
  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:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:              HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:              HKLM\software\microsoft\tracing
  Creates key:              HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:              HKCU\software\microsoft\windows nt\currentversion\winlogon
  Creates key:              HKLM\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:              HKCU\software\microsoft\windows\currentversion\internet
settings\connections
  Deletes value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]
  Deletes value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Deletes value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Deletes value:            HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\758e49c5f3fae3fd55f5c26204023b81.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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\msvcrt.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\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\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\ole32.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\comctl32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mobsync.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\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  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\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\758e49c5f3fae3fd55f5c26204023b81.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\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\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\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\{6295df2d-35ee-11d1-8707-00c04fd93327}
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}
  Opens key:                HKCU\software\classes\clsid\{6295df2d-35ee-11d1-8707-
00c04fd93327}\treatas
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\treatas
  Opens key:                HKCU\software\classes\clsid\{6295df2d-35ee-11d1-8707-
00c04fd93327}\inprocserver32
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{6295df2d-35ee-11d1-8707-
00c04fd93327}\inprocserverx86
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{6295df2d-35ee-11d1-8707-
00c04fd93327}\localserver32
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\localserver32
  Opens key:                HKCU\software\classes\clsid\{6295df2d-35ee-11d1-8707-
00c04fd93327}\inprochandler32
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{6295df2d-35ee-11d1-8707-
00c04fd93327}\inprochandlerx86
  Opens key:                HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\inprochandlerx86
  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\758e49c5f3fae3fd55f5c26204023b81.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKCU\software\classes\appid\758e49c5f3fae3fd55f5c26204023b81.exe
  Opens key:                HKCR\appid\758e49c5f3fae3fd55f5c26204023b81.exe
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\aedebug
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\winsta.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wtsapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key:                HKLM\system\setup
  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:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\faultrep.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                HKLM\software\policies\microsoft\pchealth\errorreporting
  Opens key:                HKLM\software\microsoft\pchealth\errorreporting\dw
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                HKLM\software\microsoft\mobile\sens
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  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\dwwin.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\dwwin.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\shell32.dll
  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:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\normaliz.dll
  Opens key:               HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wininet.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:               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:                HKLM\system\currentcontrolset\control\wmi\security
  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:                HKCU\software\microsoft\office\10.0\common\debug
  Opens key:                HKLM\software\microsoft\oasys\oaclient
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched20.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shfolder.dll
  Opens key:                HKLM\software\microsoft\office\10.0\common\installroot
  Opens key:                HKLM\software\microsoft\ctf\compatibility\dwwin.exe
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\psapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion
  Opens key:                HKCU\software\microsoft\internet explorer\settings
  Opens key:                HKLM\software\microsoft\pchealth\errorreporting\dw\debug
  Opens key:                HKLM\software\policies\microsoft\pchealth\errorreporting\dw
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dwwin.exe\rpcthreadpoolthrottle
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\policies
  Opens key:                HKCU\software\policies
  Opens key:                HKCU\software
  Opens key:                HKLM\software
  Opens key:                HKLM\software\policies\microsoft\internet explorer
  Opens key:                HKLM\software\policies\microsoft\internet explorer\main
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413
  Opens key:                HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\retry_headeronlypost_onconnectionreset
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                HKLM\software\microsoft\internet
```

```
explorer\main\featurecontrol\feature_bufferbreaking_818408
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_skip_post_retry_on_internetwritefile_kb895954
  Opens key:                 HKLM\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\policies\microsoft\windows\currentversion\internet
settings\5.0\cache
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_fix_chunked_proxy_script_download_kb843289
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_cname_for_spn_kb911149
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_use_spn_for_ntlm_auth_disabled
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_allow_long_international_filenames
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_permit_cache_for_authenticated_ftp_kb910274
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disallow_null_in_response_headers
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_digest_no_extras_in_uri
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_enable_passport_session_store_kb948608
  Opens key:                 HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  Opens key:                 HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_passport_check_302_for_success_kb949059
  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\dwintl.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:                HKCU\software\microsoft\windows\currentversion\internet settings\wpad
  Opens key:                HKCU\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_return_failed_connect_content_kb942615
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasman.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rtutils.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\tapi32.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\telephony
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasapi32.dll
  Opens key:                HKLM\software\microsoft\tracing\rasapi32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                HKLM\system\currentcontrolset\control\session manager\environment
  Opens key:                HKCU\environment
  Opens key:                HKCU\volatile environment
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sensapi.dll
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll
  Opens key:                HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll
  Opens key:                HKLM\system\currentcontrolset\control\securityproviders\saslprofiles
  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\software\microsoft\windows nt\currentversion\image file execution
options\msv1_0.dll
  Queries value:            HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  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[758e49c5f3fae3fd55f5c26204023b81]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[758e49c5f3fae3fd55f5c26204023b81]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  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:            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\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\software\microsoft\windows nt\currentversion\imm[ime file]
  Queries value:             HKCU\software\microsoft\ctf[disable thread input manager]
  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\{6295df2d-35ee-11d1-8707-
00c04fd93327}\localserver32[localserver32]
  Queries value:             HKCR\clsid\{6295df2d-35ee-11d1-8707-00c04fd93327}\localserver32[]
  Queries value:             HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:             HKLM\software\microsoft\ole[maximumallowedallocationsize]
  Queries value:             HKLM\software\microsoft\ole[defaultaccesspermission]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:             HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\aedebug[auto]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\aedebug[debugger]
  Queries value:             HKLM\system\setup[systemsetupinprogress]
  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:             HKLM\software\microsoft\pchealth\errorreporting[doreport]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[showui]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[allornone]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[includemicrosoftapps]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[includewindowsapps]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[dotextlog]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[includekernelfaults]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[includeshutdownerrs]
  Queries value:             HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[numberoffaultpipes]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[numberofhangpipes]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[maxuserqueuesize]
  Queries value:             HKLM\software\microsoft\pchealth\errorreporting[forcequeuemode]
  Queries value:             HKCU\control panel\desktop[lamebuttontext]
  Queries value:
HKLM\software\microsoft\pchealth\errorreporting\exclusionlist[758e49c5f3fae3fd55f5c26204023b81.exe]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  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\terminal server[tsuserenabled]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\compatibility32[dwwin]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[dwwin]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[dwwin.exe]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
```

```
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
  Queries value:              HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
  Queries value:              HKLM\software\microsoft\windows nt\currentversion\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\currentversion[programfilesdir]
  Queries value:            HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion[digitalproductid]
  Queries value:            HKCU\software\microsoft\internet explorer\settings[anchor color]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[buildpipemachine]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwfiletreeroot]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwtracking]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwnoexternalurl]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwnofilecollection]
  Queries value:
HKLM\software\microsoft\pchealth\errorreporting\dw[dwnosecondlevelcollection]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwurllaunch]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwneverupload]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwreporteename]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwnocollectionlink]
  Queries value:            HKLM\software\microsoft\pchealth\errorreporting\dw[dwallowheadless]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[fromcachetimeout]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[secureprotocols]
  Queries value:            HKLM\software\policies\microsoft\internet
explorer\main[security_hklm_only]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[certificaterevocation]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[disablekeepalive]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[disablepassport]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[idnenabled]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[cachemode]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enablehttp1_1]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyhttp1.1]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enablenegotiate]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[disablebasicoverclearchannel]
  Queries value:            HKCU\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol[feature_clientauthcertfilter]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[clientauthbuiltinui]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[syncmode5]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[sessionstarttimedefaultdeltasecs]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[signature]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[peruseritem]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\content[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[peruseritem]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\cookies[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[peruseritem]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\history[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheprefix]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cachelimit]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\domstore[cacheoptions]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacherepair]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachepath]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheprefix]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\feedplat[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\iecompat[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\ietld[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014033120140407[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\mshist012014041220140413[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacherepair]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachepath]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheprefix]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cachelimit]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache\extensible cache\privacie:[cacheoptions]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[disableworkerthreadhibernation]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[disablereadrange]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketsendbufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[socketreceivebufferlength]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[keepalivetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxhttpredirects]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperserver]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
settings[maxconnectionsper1_0server]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[maxconnectionsperproxy]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[serverinfotimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[connecttimeout]
  Queries value:              HKLM\software\microsoft\windows\currentversion\internet
```

```
settings[connecttimeout]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[connectretries]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[sendtimeout]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[receivetimeout]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[disablentlmpreauth]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[scavengecachelowerbound]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[certcachenovalidate]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelifetime]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings\5.0\cache[scavengecachefilelimit]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[httpdefaultexpirytimesecs]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[ftpdefaultexpirytimesecs]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[dwwin.exe]
  Queries value:          HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_disable_unicode_handle_closing_callback[*]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[disablecachingofsslpages]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[perusercookies]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[leashlegacycookies]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[disablent4rascheck]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[dialupuselansettings]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[sendextracrlf]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[bypassftptimecheck]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduringauth]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[releasesocketduring401auth]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[wpadsearchalldomains]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[disablelegacypreauthasserver]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasshttpnocachecheck]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[bypasssslnocachecheck]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[enablehttptrace]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[nocheckautodialoverride]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[dontusednsloadbalancing]
  Queries value:          HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:          HKCU\software\microsoft\windows\currentversion\internet
settings[mimeexclusionlistforcache]
```

```
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[headerexclusionlistforcache]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheenabled]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscacheentries]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[dnscachetimeout]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnalwaysonpost]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonzonecrossing]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertsending]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonbadcertrecving]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonpostredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[alwaysdrainonredirect]
  Queries value:              HKCU\software\microsoft\windows\currentversion\internet
settings[warnonhttpstohttpredirect]
  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:            HKCU\software\microsoft\windows\currentversion\internet
settings[globaluseroffline]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[enableautodial]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[urlencoding]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[truncatefilename]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[badproxyexpirestime]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32maxnumrequestretries]
  Queries value:
HKLM\software\microsoft\windows\currentversion\telephony[tapi32requestretrytimeout]
  Queries value:            HKLM\software\microsoft\tracing[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[enablefiletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[filetracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[enableconsoletracing]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[consoletracingmask]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[maxfilesize]
  Queries value:            HKLM\software\microsoft\tracing\rasapi32[filedirectory]
  Queries value:            HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[defaultuserprofile]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\winlogon[parseautoexec]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[migrateproxy]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyserver]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyoverride]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings[autoconfigurl]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
  Queries value:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[defaultconnectionsettings]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
  Queries value:            HKCU\software\microsoft\windows
nt\currentversion\windows[scrollinterval]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[10]
  Queries value:
HKLM\system\currentcontrolset\control\securityproviders[securityproviders]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[name]
  Queries value:
```

```
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[capabilities]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[rpcid]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[version]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msapsspc.dll[tokensize]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[name]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[capabilities]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[rpcid]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[version]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\digest.dll[tokensize]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[name]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[comment]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[capabilities]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[rpcid]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[version]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[type]
  Queries value:
HKLM\system\currentcontrolset\control\lsa\sspicache\msnsspc.dll[tokensize]
  Value changes:            HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
  Value changes:            HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
  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\explorer\shell
folders[history]
  Value changes:            HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common appdata]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings[proxyenable]
  Value changes:            HKCU\software\microsoft\windows\currentversion\internet
settings\connections[savedlegacysettings]
```