Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	736
Risk Level:	10
Date Processed:	2016-05-18 10:31:50 (UTC)
Processing Time:	61.38 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"
Sample ID:	3307
Type:	basic
Owner:	admin
Label:	6b78f38317a53920e530cc1e36053242
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	407933 bytes
MD5:	6b78f38317a53920e530cc1e36053242
SHA256:	cd43eae17643cd5510d87ca5b49ddb5b45f73b83c169dcd1102b356633943046
Description:	None

Pattern Matching Results

7	Writes to memory of system processes
2	PE: Nonstandard section
7	Injects thread into Windows process
8	Possible kernel API resolver
7	Attempts to connect to dynamic DNS
4	Reads process memory
5	PE: Contains compressed section
6	Creates ActiveSetup run key
6	Packer: PECompact
10	Creates malicious mutex: Bifrost [APT, RAT, MoreInfo]

Static Events

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

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe ["c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"]
Creates process:	C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe [c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe]
Creates process:	C:\Program Files\Internet Explorer\iexplore.exe ["C:\Program Files\Internet Explorer\IEXPLORE.EXE"]
Reads from process:	PID:1488 C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe
Reads from process:	PID:512 C:\Program Files\Internet Explorer\iexplore.exe
Reads from process:	PID:316 C:\WINDOWS\system32\calc.exe
Writes to process:	PID:1488 C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe
Writes to process:	PID:1992 C:\WINDOWS\explorer.exe
Writes to process:	PID:512 C:\Program Files\Internet Explorer\iexplore.exe
Terminates process:	C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe
Creates remote thread:	C:\WINDOWS\explorer.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\Bif1234
Creates mutex:	\BaseNamedObjects\0ok3s
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.ANH
Creates event:	\BaseNamedObjects\CTF.ThreadMarshalInterfaceEvent.000000E0.00000000.00000004
Creates event:	\BaseNamedObjects\CTF.ThreadMIConnectionEvent.000000E0.00000000.00000004
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.AO.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.AO.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.ANH.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.ANH.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

```
  Creates:                C:\Program Files\Bifrost
  Creates:                C:\Program Files\Bifrost\server.exe
  Opens:                  C:\WINDOWS\Prefetch\6B78F38317A53920E530CC1E36053-0977A58F.pf
  Opens:                  C:\Documents and Settings\Admin
  Opens:                  C:\WINDOWS\system32\winmm.dll
  Opens:                  C:\WINDOWS\system32\imm32.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\MSCTF.dll
  Opens:                  C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                  C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe
  Opens:                  C:\WINDOWS\system32\apphelp.dll
  Opens:                  C:\WINDOWS\AppPatch\sysmain.sdb
  Opens:                  C:\WINDOWS\AppPatch\systest.sdb
  Opens:                  C:\WINDOWS\Temp
  Opens:                  C:\
  Opens:                  C:\WINDOWS
  Opens:                  C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe.Manifest
  Opens:                  C:\WINDOWS\system32\shell32.dll
  Opens:                  C:\WINDOWS\system32\SHELL32.dll.124.Manifest
  Opens:                  C:\WINDOWS\system32\SHELL32.dll.124.Config
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
  Opens:                  C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
  Opens:                  C:\WINDOWS\WindowsShell.Manifest
  Opens:                  C:\WINDOWS\WindowsShell.Config
  Opens:                  C:\WINDOWS\system32\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\ws2_32.dll
  Opens:                  C:\WINDOWS\system32\ws2help.dll
  Opens:                  C:\WINDOWS\system32\advpack.dll
  Opens:                  C:\WINDOWS\system32\setupapi.dll
  Opens:                  C:\WINDOWS\system32\kernel32.dll
  Opens:                  C:\WINDOWS\system32\ntdll.dll
  Opens:                  C:\WINDOWS\system32\advapi32.dll
  Opens:                  C:\Program Files\Bifrost\server.exe
  Opens:                  C:\Program Files\Bifrost
  Opens:                  C:\Program Files\Bifrost\logg.dat
  Opens:                  C:\Program Files\Internet Explorer\iexplore.exe
  Opens:                  C:\Program Files\Internet Explorer
  Opens:                  C:\Program Files\Internet Explorer\IEXPLORE.EXE.Manifest
  Opens:                  C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
  Opens:                  C:
  Opens:                  C:\Documents and Settings
  Opens:                  C:\Documents and Settings\Admin\Cookies
  Opens:                  C:\Documents and Settings\Admin\Local Settings
  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
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\QXMNQBKF
  Opens:                  C:\Documents and Settings\Admin\Local Settings\Temporary Internet
Files\Content.IE5\UH4D6D6X
  Opens:                  C:\WINDOWS\system32\calc.exe
  Opens:                  C:\Program Files
  Opens:                  C:\WINDOWS\Registration
  Opens:                  C:\WINDOWS\system32
  Opens:                  C:\WINDOWS\system32\en-US
  Opens:                  C:\WINDOWS\WinSxS
  Opens:                  C:\WINDOWS\system32\unicode.nls
  Opens:                  C:\WINDOWS\system32\locale.nls
  Opens:                  C:\WINDOWS\system32\sorttbls.nls
  Opens:                  C:\WINDOWS\system32\rpcrt4.dll
  Opens:                  C:\WINDOWS\system32\secur32.dll
  Opens:                  C:\WINDOWS\system32\user32.dll
  Opens:                  C:\WINDOWS\system32\gdi32.dll
  Opens:                  C:\WINDOWS\system32\msvcrt.dll
  Opens:                  C:\WINDOWS\system32\shlwapi.dll
  Opens:                  C:\WINDOWS\system32\ole32.dll
  Opens:                  C:\WINDOWS\system32\iertutil.dll
  Opens:                  C:\WINDOWS\system32\urlmon.dll
  Opens:                  C:\WINDOWS\system32\oleaut32.dll
  Opens:                  C:\WINDOWS\system32\ctype.nls
  Opens:                  C:\WINDOWS\system32\sortkey.nls
  Opens:                  C:\WINDOWS\system32\ieframe.dll
```

Opens:	C:\WINDOWS\system32\en-US\ieframe.dll.mui
Opens:	C:\WINDOWS\system32\comdlg32.dll
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\Program Files\Internet Explorer\sqmapi.dll
Opens:	C:\WINDOWS\system32\winlogon.exe
Opens:	C:\WINDOWS\system32\xpsp2res.dll
Opens:	C:\WINDOWS\system32\clbcatq.dll
Opens:	C:\WINDOWS\system32\comres.dll
Opens:	C:\WINDOWS\system32\version.dll
Opens:	C:\WINDOWS\Registration\R000000000007.clb
Opens:	C:\Program Files\Internet Explorer\ieproxy.dll
Opens:	C:\WINDOWS\system32\wininet.dll
Opens:	C:\WINDOWS\system32\normaliz.dll
Opens:	C:\Documents and Settings\Admin\Local Settings\Temporary Internet Files\Content.IE5\index.dat
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\mlang.dll
Opens:	C:\WINDOWS\system32\uxtheme.dll
Opens:	C:\WINDOWS\system32\sxs.dll
Opens:	C:\WINDOWS\system32\actxprxy.dll
Opens:	C:\WINDOWS\system32\rasapi32.dll
Opens:	C:\WINDOWS\system32\rasman.dll
Opens:	C:\WINDOWS\system32\netapi32.dll
Opens:	C:\WINDOWS\system32\tapi32.dll
Opens:	C:\WINDOWS\system32\rtutils.dll
Opens:	C:\WINDOWS\system32\userenv.dll
Opens:	C:\WINDOWS\system32\sensapi.dll
Opens:	C:\WINDOWS\system32\msv1_0.dll
Opens:	C:\WINDOWS\system32\iphlpapi.dll
Opens:	C:\WINDOWS\system32\narrhook.dll
Opens:	C:\WINDOWS\system32\oleacc.dll
Opens:	C:\WINDOWS\system32\msvcp60.dll
Opens:	C:\WINDOWS\system32\oleaccrc.dll
Opens:	C:\WINDOWS\system32\MSIMTF.dll
Opens:	C:\WINDOWS\system32\stdole2.tlb
Opens:	C:\WINDOWS\system32\msimg32.dll
Opens:	C:\WINDOWS\system32\ntkrnlpa.exe
Opens:	C:\WINDOWS\system32\avicap32.dll
Opens:	C:\WINDOWS\system32\msvfw32.dll
Opens:	C:\WINDOWS\system32\mswsock.dll
Opens:	C:\WINDOWS\system32\dnsapi.dll
Opens:	C:\WINDOWS\system32\winrnr.dll
Opens:	C:\WINDOWS\system32\drivers\etc\hosts
Opens:	C:\WINDOWS\system32\rsaenh.dll
Opens:	C:\WINDOWS\system32\crypt32.dll
Opens:	C:\WINDOWS\system32\hnetcfg.dll
Opens:	C:\WINDOWS\system32\wshtcpip.dll
Opens:	C:\WINDOWS\system32\rasadhlp.dll
Writes to:	C:\Program Files\Bifrost\server.exe
Reads from:	C:\WINDOWS\Temp\6b78f38317a53920e530cc1e36053242.exe
Reads from:	C:\WINDOWS\system32\kernel32.dll
Reads from:	C:\WINDOWS\system32\ntdll.dll
Reads from:	C:\WINDOWS\system32\advapi32.dll
Reads from:	C:\WINDOWS\Prefetch\IEXPLORE.EXE-27122324.pf
Reads from:	C:\Program Files\Bifrost\server.exe
Reads from:	C:\WINDOWS\system32\calc.exe
Reads from:	C:\WINDOWS\system32\avicap32.dll
Reads from:	C:\WINDOWS\system32\drivers\etc\hosts
Reads from:	C:\WINDOWS\system32\rsaenh.dll

Network Events

DNS query:	probook.zapto.org
DNS response:	probook.zapto.org ⇒ 5.15.116.86
Connects to:	5.15.116.86:1800
Sends data to:	8.8.8.8:53
Receives data from:	0.0.0.0:0

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\internet settings
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\windows\currentversion
Creates key:	HKLM\software\microsoft\active setup\installed components\{9d71d88c-c598-4935-c5d1-43aa4db90836}
Creates key:	HKLM\software\bifrost
Creates key:	HKCU\software\bifrost
Creates key:	HKCU\sessioninformation
Creates key:	HKLM\system\currentcontrolset\control\mediaresources\msvideo
Creates key:	HKLM\system\currentcontrolset\services\tcpip\parameters

```
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6b78f38317a53920e530cc1e36053242.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.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\winmm.dll
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:                HKLM\system\currentcontrolset\control\error message instrument
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:                HKLM\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\drivers32
  Opens key:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
  Opens key:                HKCU\software\borland\locales
  Opens key:                HKLM\software\borland\locales
  Opens key:                HKCU\software\borland\delphi\locales
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\6b78f38317a53920e530cc1e36053242.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:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                HKCU\software\microsoft\ctf
  Opens key:                HKLM\software\microsoft\ctf\systemshared
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcertdlls
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:                HKLM\system\wpa\tabletpc
  Opens key:                HKLM\system\wpa\mediacenter
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\6b78f38317a53920e530cc1e36053242.exe
  Opens key:                HKLM\software\policies\microsoft\windows\safer\levelobjects
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:
```

```
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-
be2efd2c1a33}
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-
edd5fbde1328}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-
b813f72dbb91}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-
7c29ddecae3f}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-
085bcc18a68d}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-
b91490411bfc}
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
  Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll
  Opens key:                HKLM\system\setup
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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\normaliz.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:                HKCU\software\classes\
  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\software\microsoft\windows nt\currentversion\image file execution
options\wininet.dll
  Opens key:                HKLM\system\currentcontrolset\control\wmi\security
  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\setupapi.dll
  Opens key:                HKLM\system\currentcontrolset\control\minint
  Opens key:                HKLM\system\wpa\pnp
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  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\advpack.dll
  Opens key:                HKLM\software\microsoft\advanced inf setup
  Opens key:                HKLM\software\microsoft\active setup\installed components
  Opens key:                HKLM\software\microsoft\active setup\installed components\<{12d0ed0d-
0ee0-4f90-8827-78cefb8f4988}
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{26923b43-
4d38-484f-9b9e-de460746276c}
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}micros
  Opens key:                HKLM\software\microsoft\active setup\installed components\>{881dd1c5-
3dcf-431b-b061-f3f88e8be88a}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
4fcb-11cf-aaa5-00401c608500}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{10072cec-
8cc1-11d1-986e-00a0c955b42f}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{2179c5d3-
ebff-11cf-b6fd-00aa00b4e220}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{283807b5-
```

```
2c60-11d0-a31d-00aa00b92c03}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{2c7339cf-
2b09-4501-b3f3-f3508c9228ed}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{36f8ec70-
c29a-11d1-b5c7-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{3bf42070-
b3b1-11d1-b5c5-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{4278c270-
a269-11d1-b5bf-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{44bba840-
cc51-11cf-aafa-00aa00b6015c}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{44bba842-
cc51-11cf-aafa-00aa00b6015b}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{44bba848-
cc51-11cf-aafa-00aa00b6015c}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{44bba855-
cc51-11cf-aafa-00aa00b6015f}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{45ea75a0-
a269-11d1-b5bf-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{4f216970-
c90c-11d1-b5c7-0000f8051515}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{4f645220-
306d-11d2-995d-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{5945c046-
1e7d-11d1-bc44-00c04fd912be}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
3e18-11d0-821e-444553540000}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{5fd399c0-
a70a-11d1-9948-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{630b1da0-
b465-11d1-9948-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{6fab99d0-
bab8-11d1-994a-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{9381d8f2-
0288-11d0-9501-00aa00b911a5}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{acc563bc-
4266-43f0-b6ed-9d38c4202c7e}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{c09fb3cd-
3d0c-3f2d-899a-6a1d67f2073f}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{c9e9a340-
d1f1-11d0-821e-444553540600}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{cc2a9ba0-
3bdd-11d0-821e-444553540000}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{cdd7975e-
60f8-41d5-8149-19e51d6f71d0}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{d27cdb6e-
ae6d-11cf-96b8-444553540000}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{de5aed00-
a4bf-11d1-9948-00c04f98bbc9}
  Opens key:                HKLM\software\microsoft\active setup\installed components\{e92b03ab-
b707-11d2-9cbd-0000f87a369e}
  Opens key:                HKCU\software\microsoft\active setup\installed components\{9d71d88c-
c598-4935-c5d1-43aa4db90836}
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKCR\http\shell\open\command
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iexplore.exe
  Opens key:                HKCU\software\classes\applications\calc.exe
  Opens key:                HKCR\applications\calc.exe
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\fileassociation
  Opens key:                HKLM\software\microsoft\ctf\tip\
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
  Opens key:                HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}
  Opens key:                HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
```

```
c9633f71be64}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{1188450c-fdab-47ae-80d8-
c9633f71be64}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  Opens key:                 HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}
  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\iexplore.exe\rpcthreadpoolthrottle
  Opens key:                 HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                 HKLM\software\microsoft\ctf\compatibility\iexplore.exe
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvfw32.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\vfw
  Opens key:                 HKLM\system\currentcontrolset\control\mediaresources\msvideo
  Opens key:                 HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dnsapi.dll
  Opens key:                 HKLM\system\currentcontrolset\services\dnscache\parameters
  Opens key:                 HKLM\software\policies\microsoft\windows nt\dnsclient
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iphlpapi.dll
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\linkage
  Opens key:                 HKLM\system\currentcontrolset\services\tcpip\parameters\
  Opens key:                 HKLM\system\currentcontrolset\services\netbt\parameters\interfaces
  Opens key:                 HKLM\system\currentcontrolset\services\netbt\parameters
  Opens key:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wldap32.dll
```

```
  Opens key:                HKLM\system\currentcontrolset\services\ldap
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winrnr.dll
  Opens key:                HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rsaenh.dll
  Opens key:                HKLM\software\policies\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography
  Opens key:                HKLM\software\microsoft\cryptography\offload
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rasadhlp.dll
  Opens key:                HKCU\appevents\schemes\apps\.default\systemnotification\.current
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\treatas
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\treatas
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserver32
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprocserverx86
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver32
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver32
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandler32
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\inprochandlerx86
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{ba126ae5-2166-11d1-b1d0-
00805fc1270e}\localserver
  Opens key:                HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}\localserver
  Opens key:                HKCU\software\classes\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
  Opens key:                HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\treatas
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\treatas
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserver32
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserverx86
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\localserver32
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver32
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandler32
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprochandlerx86
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\localserver
  Opens key:                HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\localserver
  Opens key:                HKCU\software\policies\microsoft\windows\network connections
  Opens key:                HKLM\software\policies\microsoft\windows\network connections
  Opens key:                HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder
  Opens key:                HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\nonenum
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{2227a280-3aea-1069-
a2de-08002b30309d}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}\shellfolder
```

```
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{2227a280-
3aea-1069-a2de-08002b30309d}\shellfolder
  Opens key:                 HKCU\software\classes\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
  Opens key:                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}
  Opens key:                 HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}\
  Opens key:                 HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder
  Opens key:                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\shellfolder
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{7007acc7-3202-11d1-
aad2-00805fc1270e}
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}\shellfolder
  Opens key:                 HKLM\software\microsoft\windows\currentversion\explorer\clsid\{7007acc7-
3202-11d1-aad2-00805fc1270e}\shellfolder
  Opens key:                 HKCU\software\classes\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
  Opens key:                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}
  Opens key:                 HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}\
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:             HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\compatibility32[6b78f38317a53920e530cc1e36053242]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[6b78f38317a53920e530cc1e36053242]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:             HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:             HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:             HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:             HKCR\interface[interfacehelperdisableall]
  Queries value:             HKCR\interface[interfacehelperdisableallforole32]
  Queries value:             HKCR\interface[interfacehelperdisabletypelib]
  Queries value:             HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:             HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:             HKCU\control panel\desktop[multiuilanguageid]
  Queries value:             HKCU\control panel\desktop[smoothscroll]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
  Queries value:
HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
  Queries value:            HKLM\software\microsoft\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\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\setup[systemsetupinprogress]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[6b78f38317a53920e530cc1e36053242.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:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  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\control\computername\activecomputername[computername]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
  Queries value:            HKLM\software\microsoft\advanced inf setup[advpacklogfile]
  Queries value:            HKLM\software\microsoft\active setup\installed components\<{12d0ed0d-
0ee0-4f90-8827-78cefb8f4988}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\>{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\>{26923b43-
4d38-484f-9b9e-de460746276c}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\>{60b49e34-
c7cc-11d0-8953-00a0c90347ff}micros[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\>{881dd1c5-
3dcf-431b-b061-f3f88e8be88a}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{08b0e5c0-
4fcb-11cf-aaa5-00401c608500}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{10072cec-
8cc1-11d1-986e-00a0c955b42f}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{2179c5d3-
ebff-11cf-b6fd-00aa00b4e220}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{22d6f312-
b0f6-11d0-94ab-0080c74c7e95}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{283807b5-
2c60-11d0-a31d-00aa00b92c03}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{2c7339cf-
2b09-4501-b3f3-f3508c9228ed}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{36f8ec70-
c29a-11d1-b5c7-0000f8051515}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{3af36230-
a269-11d1-b5bf-0000f8051515}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{3bf42070-
b3b1-11d1-b5c5-0000f8051515}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{4278c270-
a269-11d1-b5bf-0000f8051515}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{44bba840-
cc51-11cf-aafa-00aa00b6015c}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{44bba842-
cc51-11cf-aafa-00aa00b6015b}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{44bba848-
cc51-11cf-aafa-00aa00b6015c}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{44bba855-
cc51-11cf-aafa-00aa00b6015f}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{45ea75a0-
a269-11d1-b5bf-0000f8051515}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{4f216970-
c90c-11d1-b5c7-0000f8051515}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{4f645220-
306d-11d2-995d-00c04f98bbc9}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{5945c046-
1e7d-11d1-bc44-00c04fd912be}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{5a8d6ee0-
3e18-11d0-821e-444553540000}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{5fd399c0-
a70a-11d1-9948-00c04f98bbc9}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{630b1da0-
b465-11d1-9948-00c04f98bbc9}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{6bf52a52-
394a-11d3-b153-00c04f79faa6}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{6fab99d0-
bab8-11d1-994a-00c04f98bbc9}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{7790769c-
0471-11d2-af11-00c04fa35d02}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4340}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{89820200-
ecbd-11cf-8b85-00aa005b4383}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{89b4c1cd-
b018-4511-b0a1-5476dbf70820}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{9381d8f2-
0288-11d0-9501-00aa00b911a5}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{acc563bc-
4266-43f0-b6ed-9d38c4202c7e}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{c09fb3cd-
3d0c-3f2d-899a-6a1d67f2073f}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{c9e9a340-
d1f1-11d0-821e-444553540600}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{cc2a9ba0-
3bdd-11d0-821e-444553540000}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{cdd7975e-
60f8-41d5-8149-19e51d6f71d0}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{d27cdb6e-
ae6d-11cf-96b8-444553540000}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{de5aed00-
a4bf-11d1-9948-00c04f98bbc9}[stubpath]
  Queries value:            HKLM\software\microsoft\active setup\installed components\{e92b03ab-
b707-11d2-9cbd-0000f87a369e}[stubpath]
  Queries value:            HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:            HKLM\software\bifrost[nck]
  Queries value:            HKCR\http\shell\open\command[]
  Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\fileassociation[cutlist]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{246ecb87-c2f2-4abe-905b-c8b38add2c43}[dword]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{34745c63-b2f0-4784-8b67-5e12c8701a31}[dword]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{5130a009-5540-4fcf-97eb-aad33fc0ee09}[dword]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{7ae86bb7-262c-431e-9111-c974b6b7cac3}[dword]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{b5a73cd1-8355-426b-a161-259808f26b14}[dword]
  Queries value:            HKLM\software\microsoft\ctf\tip\{78cb5b0e-26ed-4fcc-854c-
77e8f3d1aa80}\category\item\{c6debc0a-f2b2-4f17-930e-ca9faff4cd04}[dword]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\compatibility32[iexplore]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[iexplore]
  Queries value:            HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[iexplore.exe]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:            HKCU\software\bifrost[plg1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo1]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo2]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo3]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo4]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo5]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo6]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo8]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\drivers32[msvideo9]
  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[enableautodial]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryadaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disableadapterdomainname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[usedomainnamedevolution]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[prioritizerecorddata]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[allowunqualifiedquery]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[appendtomultilabelname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenbadtlds]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[screenunreachableservers]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[filterclusterip]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[waitfornameerroronall]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[useedns]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[queryipmatching]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[usehostsfile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationenabled]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disabledynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerprimaryname]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registeradaptername]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[enableadapterdomainnameregistration]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerreverselookup]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablereverseaddressregistrations]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registerwanadapters]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[disablewandynamicupdate]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationttl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[defaultregistrationrefreshinterval]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[registrationmaxaddresscount]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[maxnumberofaddressestoregister]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[updatesecuritylevel]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatezoneexcludefile]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[updatetopleveldomainzones]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[dnstest]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachesize]
   Queries value:              HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxnegativecachettl]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[adaptertimeoutlimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[serverprioritytimelimit]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[maxcachedsockets]
   Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastlistenlevel]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\dnscache\parameters[multicastsendlevel]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsquickquerytimeouts]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsmulticastquerytimeouts]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\linkage[bind]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[enabledhcp]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseobtainedtime]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[leaseterminatestime]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[queryadaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[disableadapterdomainname]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registeradaptername]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[registrationmaxaddresscount]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[maxnumberofaddressestoregister]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[domain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpdomain]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[ipautoconfigurationenabled]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[addresstype]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[nameserver]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\interfaces\{16325b0b-4636-4303-abe3-
c7d49d7cecdc}[dhcpnameserver]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters[searchlist]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters[dnsnbtlookuporder]
  Queries value:            HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[type]
  Queries value:            HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong
cryptographic provider[image path]
  Queries value:            HKLM\software\microsoft\cryptography[machineguid]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
  Queries value:            HKLM\system\currentcontrolset\services\winsock2\parameters[autodialdll]
  Queries value:            HKCU\appevents\schemes\apps\.default\systemnotification\.current[]
  Queries value:            HKLM\software\microsoft\com3[regdbversion]
  Queries value:            HKCR\clsid\{ba126ae5-2166-11d1-b1d0-00805fc1270e}[appid]
  Queries value:            HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[dllsurrogate]
  Queries value:            HKCR\appid\{27af75ed-20d9-11d1-b1ce-00805fc1270e}[localservice]
```

```
   Queries value:               HKCR\clsid\{33c4643c-7811-46fa-a89a-
768597bd7223}\inprocserver32[inprocserver32]
   Queries value:               HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}\inprocserver32[]
   Queries value:               HKCR\clsid\{33c4643c-7811-46fa-a89a-768597bd7223}[appid]
   Queries value:               HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[wantsfordisplay]
   Queries value:               HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[attributes]
   Queries value:               HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[callforattributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{2227a280-3aea-1069-a2de-
08002b30309d}]
   Queries value:               HKCR\clsid\{2227a280-3aea-1069-a2de-
08002b30309d}\shellfolder[hidefolderverbs]
   Queries value:               HKCR\clsid\{2227a280-3aea-1069-a2de-08002b30309d}[localizedstring]
   Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9319]
   Queries value:               HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[wantsfordisplay]
   Queries value:               HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[attributes]
   Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{7007acc7-3202-11d1-aad2-
00805fc1270e}]
   Queries value:               HKCR\clsid\{7007acc7-3202-11d1-aad2-
00805fc1270e}\shellfolder[hidefolderverbs]
   Queries value:               HKCR\clsid\{7007acc7-3202-11d1-aad2-00805fc1270e}[localizedstring]
   Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\netshell.dll,-1200]
   Sets/Creates value:          HKLM\software\microsoft\active setup\installed components\{9d71d88c-
c598-4935-c5d1-43aa4db90836}[stubpath]
   Sets/Creates value:          HKLM\software\bifrost[nck]
   Sets/Creates value:          HKCU\software\bifrost[klg]
   Sets/Creates value:
HKCU\software\microsoft\windows\shellnoroam\muicache[c:\windows\system32\calc.exe]
   Value changes:               HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:               HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
   Value changes:               HKCU\sessioninformation[programcount]
   Value changes:               HKLM\software\microsoft\active setup\installed components\{9d71d88c-
c598-4935-c5d1-43aa4db90836}[stubpath]
```