Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	820
Risk Level:	6
Date Processed:	2016-05-18 10:42:11 (UTC)
Processing Time:	63.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe"
Sample ID:	3328
Type:	basic
Owner:	admin
Label:	6ff8b3dc9a34dc40e47ff4c3444c8241
Date Added:	2016-05-18 10:30:51 (UTC)
File Type:	PE32:win32:gui
File Size:	394240 bytes
MD5:	6ff8b3dc9a34dc40e47ff4c3444c8241
SHA256:	22dd9934836541b81983ef5ed7abb4d82edd6afcdc272f027f8bffb41145fac9
Description:	None

Pattern Matching Results

6	Modifies registry autorun entries
2	PE: Nonstandard section
6	Creates executable in application data folder
3	Long sleep detected
5	PE: Contains compressed section
5	Adds autostart object

Static Events

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

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe ["c:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.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\7CDE0514E17F2F6600007CDD883D3542
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates:	C:\Documents and Settings\All Users\Application Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542
Creates:	C:\Documents and Settings\All Users\Application Data\7CDE0514E17F2F6600007CDD883D3542
Creates:	C:\Documents and Settings\All Users\Application Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542.exe
Creates:	C:\Documents and Settings\All Users\Application Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542.ico
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\crypt32.dll
Opens:	C:\WINDOWS\system32\msasn1.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\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\activeds.dll
  Opens:                    C:\WINDOWS\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens:                    C:\WINDOWS\system32\psapi.dll
  Opens:                    C:\WINDOWS\system32\msimg32.dll
  Opens:                    C:\WINDOWS\system32\winhttp.dll
  Opens:                    C:\WINDOWS\system32\rpcss.dll
  Opens:                    C:\WINDOWS\system32\MSCTF.dll
  Opens:                    C:\
  Opens:                    C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542
  Opens:                    C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542\
  Opens:                    C:\Documents and Settings\All Users\Application Data
  Opens:                    C:\WINDOWS\system32\ws2_32.dll
  Opens:                    C:\WINDOWS\system32\ws2help.dll
  Opens:                    C:\WINDOWS\system32\mswsock.dll
  Opens:                    C:\WINDOWS\system32\hnetcfg.dll
  Opens:                    C:\WINDOWS\system32\wshtcpip.dll
  Opens:                    C:\windows\temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  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\sxs.dll
  Opens:                    C:\WINDOWS\system32\ieframe.dll
  Opens:                    C:\WINDOWS\system32\stdole2.tlb
  Opens:                    C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                    C:\WINDOWS\system32\MSIMTF.dll
  Opens:                    C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542.exe
  Opens:                    C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542
  Opens:                    C:\WINDOWS\Fonts\arialbd.ttf
  Opens:                    C:\Program Files\Internet Explorer\iexplore.exe
  Opens:                    C:\WINDOWS\system32\ieframe.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\ieframe.dll.123.Config
  Opens:                    C:\WINDOWS\system32\en-US\ieframe.dll.mui
  Opens:                    C:\WINDOWS\Temp\df94a9e0-9251-40e1-82b1-cbd379a56d17
  Writes to:                C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542.exe
  Writes to:                C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542
  Writes to:                C:\Documents and Settings\All Users\Application
Data\7CDE0514E17F2F6600007CDD883D3542\7CDE0514E17F2F6600007CDD883D3542.ico
  Reads from:               C:\WINDOWS\system32\activeds.dll
  Reads from:               C:\WINDOWS\Temp\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Reads from:               C:\WINDOWS\Registration\R000000000007.clb
  Reads from:               C:\WINDOWS\system32\ieframe.dll
  Reads from:               C:\WINDOWS\system32\stdole2.tlb
```

Network Events

```
  Connects to:              175.41.29.181:80
  Sends data to:            175.41.29.181:80
```

Windows Registry Events

```
  Creates key:              HKCU\software\microsoft\windows\currentversion\runonce
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\6ff8b3dc9a34dc40e47ff4c3444c8241.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\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\msvcrt.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\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\msasn1.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.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\shlwapi.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\comdlg32.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\system\currentcontrolset\services\crypt32\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\msasn1
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\performance
  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\psapi.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\msimg32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKCR\interface
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\winhttp.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\tracing
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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
  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\6ff8b3dc9a34dc40e47ff4c3444c8241.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:                HKLM\system\currentcontrolset\control\computername\activecomputername
  Opens key:                HKLM\software\microsoft\internet explorer
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet settings\winhttp
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\connections
  Opens key:                HKLM\software\microsoft\windows\currentversion\internet
settings\winhttp\unsafesslapps
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\ws2_32.dll
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\mswsock.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\hnetcfg.dll
  Opens key:                HKLM\software\microsoft\rpc\securityservice
  Opens key:                HKLM\system\currentcontrolset\services\winsock\parameters
  Opens key:                HKLM\system\currentcontrolset\services\tcpip\parameters\winsock
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wshtcpip.dll
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKCU\software\classes\
  Opens key:                HKLM\software\classes
  Opens key:                HKU\
  Opens key:                HKCR\clsid
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\treatas
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\treatas
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserverx86
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\localserver32
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver32
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandler32
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprochandlerx86
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\localserver
```

```
  Opens key:                HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\localserver
  Opens key:                HKCU\software\classes\appid\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens key:                HKCR\appid\6ff8b3dc9a34dc40e47ff4c3444c8241.exe
  Opens key:                HKLM\system\currentcontrolset\control\lsa
  Opens key:                HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
  Opens key:                HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}
  Opens key:                HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\proxystubclsid32
  Opens key:                HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\treatas
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\treatas
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserverx86
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\localserver32
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\localserver32
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\inprochandlerx86
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{00020424-0000-0000-c000-
000000000046}\localserver
  Opens key:                HKCR\clsid\{00020424-0000-0000-c000-000000000046}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\xpsp2res.dll
  Opens key:                HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\forward
  Opens key:                HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\forward
  Opens key:                HKCU\software\classes\interface\{85cb6900-4d95-11cf-960c-
0080c7f4ee85}\typelib
  Opens key:                HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib
  Opens key:                HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
  Opens key:                HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}
  Opens key:                HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:                HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1
  Opens key:                HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0
  Opens key:                HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0
  Opens key:                HKCU\software\classes\typelib\{eab22ac0-30c1-11cf-a7eb-
0000c05bae0b}\1.1\0\win32
  Opens key:                HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32
  Opens key:                HKCU\software\classes\typelib
  Opens key:                HKCR\typelib
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0
  Opens key:                HKCU\software\classes\typelib\{00020430-0000-0000-c000-
000000000046}\2.0\0\win32
  Opens key:                HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32
  Opens key:                HKCU\software\classes\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\interface\{00020400-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\treatas
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\treatas
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserverx86
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\localserver32
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\localserver32
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandler32
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\inprochandlerx86
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{00020420-0000-0000-c000-
000000000046}\localserver
  Opens key:                HKCR\clsid\{00020420-0000-0000-c000-000000000046}\localserver
  Opens key:                HKCU\software\classes\interface\{b196b284-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCR\interface\{b196b284-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCU\software\classes\interface\{b196b284-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32
  Opens key:                HKCR\interface\{b196b284-bab4-101a-b69c-00aa00341d07}\proxystubclsid32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\treatas
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\treatas
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserverx86
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\localserver32
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\localserver32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandler32
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprochandlerx86
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\localserver
  Opens key:                HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\localserver
  Opens key:                HKCU\software\classes\interface\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCR\interface\{b196b286-bab4-101a-b69c-00aa00341d07}
  Opens key:                HKCU\software\classes\interface\{b196b286-bab4-101a-b69c-
00aa00341d07}\proxystubclsid32
  Opens key:                HKCR\interface\{b196b286-bab4-101a-b69c-00aa00341d07}\proxystubclsid32
  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\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\treatas
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\treatas
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserverx86
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandler32
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprochandlerx86
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\localserver
  Opens key:                HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\iertutil.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ieframe.dll
  Opens key:                HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe
  Opens key:                HKLM\software\microsoft\internet explorer\setup
  Opens key:                HKLM\system\currentcontrolset\control\wmi\security
  Opens key:                HKCU\software\classes\interface\{eab22ac1-30c1-11cf-a7eb-
0000c05bae0b}\typelib
  Opens key:                HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib
  Opens key:                HKCU\software\classes\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                HKCR\clsid\{a4a1a128-768f-41e0-bf75-e4fddd701cba}
  Opens key:                HKCU\software\classes\interface\{b722bccb-4e68-101b-a2bc-
00aa00404770}\proxystubclsid32
  Opens key:                HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{79eac9c4-baf9-11ce-8c82-
00aa004ba90b}\proxystubclsid32
  Opens key:                HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{000214e6-0000-0000-c000-
000000000046}\proxystubclsid32
  Opens key:                HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32
  Opens key:                HKCU\software\classes\interface\{93f2f68c-1d1b-11d3-a30e-
00c04f79abd1}\proxystubclsid32
  Opens key:                HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32
  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\terminal server[tsuserenabled]
  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[6ff8b3dc9a34dc40e47ff4c3444c8241]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[6ff8b3dc9a34dc40e47ff4c3444c8241]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:            HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:            HKCR\interface[interfacehelperdisableall]
  Queries value:            HKCR\interface[interfacehelperdisableallforole32]
  Queries value:            HKCR\interface[interfacehelperdisabletypelib]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:            HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:            HKCU\keyboard layout\toggle[language hotkey]
  Queries value:            HKCU\keyboard layout\toggle[hotkey]
  Queries value:            HKCU\keyboard layout\toggle[layout hotkey]
  Queries value:            HKLM\software\microsoft\ctf[enableanchorcontext]
  Queries value:            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[profilesdirectory]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
  Queries value:            HKLM\software\microsoft\rpc[maxrpcsize]
  Queries value:
HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
  Queries value:            HKLM\software\microsoft\internet explorer[version]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings[sharecredswithwinhttp]
  Queries value:            HKLM\software\microsoft\windows\currentversion\internet
settings\connections[winhttpsettings]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[next_catalog_entry_id]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003[packedcatalogitem]
```

```
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[librarypath]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[displaystring]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerid]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[enabled]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[storesserviceclassinfo]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets]
  Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount]
  Queries value:            HKLM\software\microsoft\rpc\securityservice[defaultauthlevel]
  Queries value:            HKLM\system\currentcontrolset\services\winsock\parameters[transports]
  Queries value:            HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[mapping]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[minsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[maxsockaddrlength]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[usedelayedacceptance]
  Queries value:
HKLM\system\currentcontrolset\services\tcpip\parameters\winsock[helperdllname]
```

```
   Queries value:               HKLM\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\{9ba05972-f6a8-11cf-a442-
00a0c90a8f39}\inprocserver32[inprocserver32]
   Queries value:               HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}\inprocserver32[]
   Queries value:               HKCR\clsid\{9ba05972-f6a8-11cf-a442-00a0c90a8f39}[appid]
   Queries value:               HKLM\software\microsoft\ole[maximumallowedallocationsize]
   Queries value:               HKLM\software\microsoft\ole[defaultaccesspermission]
   Queries value:               HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
   Queries value:               HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\proxystubclsid32[]
   Queries value:               HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
   Queries value:               HKCR\clsid\{00020424-0000-0000-c000-000000000046}\inprocserver32[]
   Queries value:               HKCR\clsid\{00020424-0000-0000-c000-000000000046}[appid]
   Queries value:               HKCR\clsid\{00020424-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
   Queries value:               HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[]
   Queries value:               HKCR\interface\{85cb6900-4d95-11cf-960c-0080c7f4ee85}\typelib[version]
   Queries value:               HKCR\typelib\{eab22ac0-30c1-11cf-a7eb-0000c05bae0b}\1.1\0\win32[]
   Queries value:               HKCR\typelib\{00020430-0000-0000-c000-000000000046}\2.0\0\win32[]
   Queries value:               HKLM\software\microsoft\rpc[udtalignmentpolicy]
   Queries value:               HKCR\interface\{00020400-0000-0000-c000-000000000046}\proxystubclsid32[]
   Queries value:               HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[inprocserver32]
   Queries value:               HKCR\clsid\{00020420-0000-0000-c000-000000000046}\inprocserver32[]
   Queries value:               HKCR\clsid\{00020420-0000-0000-c000-000000000046}[appid]
   Queries value:               HKCR\clsid\{00020420-0000-0000-c000-
000000000046}\inprocserver32[threadingmodel]
   Queries value:               HKCR\interface\{b196b284-bab4-101a-b69c-00aa00341d07}\proxystubclsid32[]
   Queries value:               HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[inprocserver32]
   Queries value:               HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}\inprocserver32[]
   Queries value:               HKCR\clsid\{b196b286-bab4-101a-b69c-00aa00341d07}[appid]
   Queries value:               HKCR\clsid\{b196b286-bab4-101a-b69c-
00aa00341d07}\inprocserver32[threadingmodel]
   Queries value:               HKCR\interface\{b196b286-bab4-101a-b69c-00aa00341d07}\proxystubclsid32[]
   Queries value:               HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
   Queries value:               HKCU\software\microsoft\ctf[disable thread input manager]
   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[arial]
   Queries value:               HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[inprocserver32]
   Queries value:               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}\inprocserver32[]
   Queries value:               HKCR\clsid\{8856f961-340a-11d0-a96b-00c04fd705a2}[appid]
   Queries value:               HKCR\clsid\{8856f961-340a-11d0-a96b-
00c04fd705a2}\inprocserver32[threadingmodel]
   Queries value:               HKLM\software\microsoft\windows\currentversion\app paths\iexplore.exe[]
   Queries value:               HKLM\software\microsoft\internet explorer\setup[iexplorelastmodifiedlow]
   Queries value:               HKLM\software\microsoft\internet
explorer\setup[iexplorelastmodifiedhigh]
   Queries value:               HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
   Queries value:               HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
   Queries value:               HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
   Queries value:               HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
   Queries value:               HKLM\software\microsoft\internet explorer\setup[installstarted]
   Queries value:               HKCR\interface\{b722bccb-4e68-101b-a2bc-00aa00404770}\proxystubclsid32[]
   Queries value:               HKCR\interface\{79eac9c4-baf9-11ce-8c82-00aa004ba90b}\proxystubclsid32[]
   Queries value:               HKCR\interface\{000214e6-0000-0000-c000-000000000046}\proxystubclsid32[]
   Queries value:               HKCR\interface\{93f2f68c-1d1b-11d3-a30e-00c04f79abd1}\proxystubclsid32[]
   Sets/Creates value:
HKCU\software\microsoft\windows\currentversion\runonce[7cde0514e17f2f6600007cdd883d3542]
   Value changes:               HKLM\software\microsoft\cryptography\rng[seed]
```