Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 69, Task ID: 275

Task ID:	275
Risk Level:	1
Date Processed:	2016-04-28 12:54:42 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\1e582d1e5a53441b694d7073a8bbc09c.exe"

Sample ID:	69
Type:	basic
Owner:	admin
Label:	1e582d1e5a53441b694d7073a8bbc09c
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	60928 bytes
MD5:	1e582d1e5a53441b694d7073a8bbc09c
SHA256:	b4effd7c5bca3871fc19cbf1e132d2a877f6b20278fd21031a85de762ddddb6a
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\1e582d1e5a53441b694d7073a8bbc09c.exe ["c:\windows\temp\1e582d1e5a53441b694d7073a8bbc09c.exe"]

Named Object Events

Creates mutex:	\BaseNamedObjects\SendToMD5Instance
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\Shell.CMruPidlList
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.MN
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.EGD
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates event:	\BaseNamedObjects\MSCTF.SendReceive.Event.EGD.IC
Creates event:	\BaseNamedObjects\MSCTF.SendReceiveConection.Event.EGD.IC
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{090851A5-EB96-11D2-8BE4-00C04FA31A66}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Opens:	C:\WINDOWS\Prefetch\1E582D1E5A53441B694D7073A8BBC-01FCFB14.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config

```
  Opens:                    C:\WINDOWS\system32\uxtheme.dll
  Opens:                    C:\WINDOWS\Temp
  Opens:                    C:\windows\temp\1e582d1e5a53441b694d7073a8bbc09c.ini
  Opens:                    C:\WINDOWS\system32\MSCTF.dll
  Opens:                    C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                    C:\WINDOWS\system32\ole32.dll
  Opens:                    C:\WINDOWS\system32\MSIMTF.dll
  Opens:                    C:\WINDOWS\system32\rpcss.dll
  Opens:                    C:\WINDOWS\system32\cscui.dll
  Opens:                    C:\WINDOWS\system32\clbcatq.dll
  Opens:                    C:\WINDOWS\system32\comres.dll
  Opens:                    C:\WINDOWS\Registration\R000000000007.clb
  Opens:                    C:\WINDOWS\system32\cscdll.dll
  Opens:                    C:\WINDOWS\System32\cscui.dll.124.Manifest
  Opens:                    C:\WINDOWS\System32\cscui.dll.124.Config
  Opens:                    C:\WINDOWS\system32\browseui.dll
  Opens:                    C:\WINDOWS\system32\browseui.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\browseui.dll.123.Config
  Opens:                    C:\WINDOWS\system32\setupapi.dll
  Opens:                    C:\
  Opens:                    C:\Documents and Settings
  Opens:                    C:\Documents and Settings\Admin\Local Settings
  Opens:                    C:\Documents and Settings\Admin\My Documents\desktop.ini
  Opens:                    C:\WINDOWS\system32\ntshrui.dll
  Opens:                    C:\WINDOWS\system32\atl.dll
  Opens:                    C:\WINDOWS\system32\netapi32.dll
  Opens:                    C:\WINDOWS\system32\ntshrui.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\ntshrui.dll.123.Config
  Opens:                    C:\WINDOWS\system32\mydocs.dll
  Opens:                    C:\Documents and Settings\Admin\Recent\Desktop.ini
  Opens:                    C:\Documents and Settings\Admin\My Documents
  Opens:                    C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
  Opens:                    C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
  Opens:                    C:\WINDOWS\system32\shdocvw.dll
  Opens:                    C:\WINDOWS\system32\crypt32.dll
  Opens:                    C:\WINDOWS\system32\msasn1.dll
  Opens:                    C:\WINDOWS\system32\cryptui.dll
  Opens:                    C:\WINDOWS\system32\CRYPTUI.dll.2.Manifest
  Opens:                    C:\WINDOWS\system32\CRYPTUI.dll.2.Config
  Opens:                    C:\WINDOWS\system32\wintrust.dll
  Opens:                    C:\WINDOWS\system32\urlmon.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\urlmon.dll.123.Config
  Opens:                    C:\WINDOWS\system32\WININET.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\WININET.dll.123.Config
  Opens:                    C:\WINDOWS\system32\riched20.dll
  Opens:                    C:\WINDOWS\system32\shdocvw.dll.123.Manifest
  Opens:                    C:\WINDOWS\system32\shdocvw.dll.123.Config
  Opens:                    C:\Documents and Settings\Admin\Favorites\Desktop.ini
  Reads from:               C:\WINDOWS\Registration\R000000000007.clb
  Reads from:               C:\WINDOWS\system32\shell32.dll
  Reads from:               C:\Documents and Settings\Admin\My Documents\desktop.ini
  Reads from:               C:\WINDOWS\system32\mydocs.dll
  Reads from:               C:\Documents and Settings\Admin\Recent\Desktop.ini
  Reads from:               C:\Documents and Settings\Admin\My Documents\My Music\Desktop.ini
  Reads from:               C:\Documents and Settings\Admin\My Documents\My Pictures\Desktop.ini
  Reads from:               C:\Documents and Settings\Admin\Favorites\Desktop.ini
```

Windows Registry Events

```
  Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}\
  Creates key:              HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru\
  Creates key:              HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:              HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:              HKCU\software\microsoft\windows\currentversion\internet settings
  Creates key:              HKCU\software\microsoft\windows\shellnoroam\bagmru
  Creates key:              HKCU\software\microsoft\windows\shellnoroam\bagmru\3
  Creates key:              HKCU\software\microsoft\windows\shellnoroam\bags\22\shell
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
```

```
options\1e582d1e5a53441b694d7073a8bbc09c.exe
  Opens key:                HKLM\system\currentcontrolset\control\terminal server
  Opens key:
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:                HKLM\system\currentcontrolset\control\safeboot\option
  Opens key:                HKLM\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKCU\software\policies\microsoft\windows\safer\codeidentifiers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\user32.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\software\microsoft\windows\currentversion\explorer\performance
  Opens key:                HKCU\
  Opens key:                HKCU\software\policies\microsoft\control panel\desktop
  Opens key:                HKCU\control panel\desktop
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\languagepack
  Opens key:                HKLM\system\setup
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\thememanager
  Opens key:                HKCU\software\vaultec\sendtomd5
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\1e582d1e5a53441b694d7073a8bbc09c.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                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:                HKCU\software\microsoft\ctf
  Opens key:                HKLM\software\microsoft\ctf\systemshared
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                HKCU\software\microsoft\ctf\langbaraddin\
  Opens key:                HKLM\software\microsoft\ctf\langbaraddin\
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\
  Opens key:                HKCU\control panel\desktop\windowmetrics
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\shell icons
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers
  Opens key:
HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline files
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\apphelp.dll
  Opens key:                HKLM\system\currentcontrolset\control\session manager\appcompatibility
  Opens key:                HKLM\software\microsoft\com3
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comres.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:                HKLM\software\microsoft\oleaut
  Opens key:                HKLM\software\microsoft\oleaut\userera
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\clbcatq.dll
  Opens key:                HKLM\software\microsoft\com3\debug
  Opens key:                HKLM\software\classes
  Opens key:                HKU\
  Opens key:                HKCR\clsid
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\treatas
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\treatas
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserverx86
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\localserver32
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver32
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprochandler32
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprochandlerx86
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\localserver
  Opens key:                HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cscdll.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\cscui.dll
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\system
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\treatas
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\treatas
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\inprocserverx86
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\localserver32
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\localserver32
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\inprochandler32
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\inprochandlerx86
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\localserver
  Opens key:                HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\localserver
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\browseui.dll
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\1e582d1e5a53441b694d7073a8bbc09c.exe
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\comdlg32
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\comdlg32
  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\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\1e582d1e5a53441b694d7073a8bbc09c.exe\rpcthreadpoolthrottle
  Opens key:                HKLM\software\policies\microsoft\windows nt\rpc
  Opens key:                HKLM\system\currentcontrolset\control\computername
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\autocomplete
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\treatas
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\treatas
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserverx86
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\localserver32
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver32
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprochandler32
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprochandlerx86
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\localserver
  Opens key:                HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\localserver
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{03c036f1-a186-11d0-
824a-00aa005b4383}
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\treatas
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\treatas
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserverx86
```

```
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\localserver32
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver32
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandler32
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprochandlerx86
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\localserver
  Opens key:                HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\localserver
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{00bb2763-6a77-11d0-
a535-00c04fd7d062}
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:                HKLM\system\currentcontrolset\control\productoptions
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:                HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder
  Opens key:                HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
  Opens key:                HKCU\software\classes\clsid\{20d04fe0-3aea-1069-a2d8-
08002b30309d}\inprocserver32
  Opens key:                HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32
  Opens key:                HKCU\software\classes\directory
  Opens key:                HKCR\directory
  Opens key:                HKCU\software\classes\directory\curver
  Opens key:                HKCR\directory\curver
  Opens key:                HKCR\directory\
  Opens key:                HKCU\software\classes\directory\shellex\iconhandler
  Opens key:                HKCR\directory\shellex\iconhandler
  Opens key:                HKCU\software\classes\directory\clsid
  Opens key:                HKCR\directory\clsid
  Opens key:                HKCU\software\classes\folder
  Opens key:                HKCR\folder
  Opens key:                HKCU\software\classes\folder\clsid
  Opens key:                HKCR\folder\clsid
  Opens key:                HKCU\software\classes\network\sharinghandler
  Opens key:                HKCR\network\sharinghandler
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\atl.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\netapi32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntshrui.dll
  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\{450d8fba-ad25-11d0-
98a8-0800361b1103}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\shellfolder
  Opens key:                HKLM\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\shellfolder
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\shellex\iconhandler
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\defaulticon
  Opens key:                HKCU\software\classes\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}
  Opens key:                HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}
  Opens key:                HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\
  Opens key:                HKCU\software\microsoft\windows\shellnoroam
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\muicache\
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\streams\defaults
  Opens key:                HKCU\software\microsoft\internet explorer\main
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\treatas
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\treatas
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\inprocserver32
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\inprocserver32
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\inprocserverx86
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\inprocserverx86
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\localserver32
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\localserver32
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\inprochandler32
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\inprochandler32
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\inprochandlerx86
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\inprochandlerx86
  Opens key:                HKCU\software\classes\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\localserver
  Opens key:                HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\localserver
  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\system\currentcontrolset\services\crypt32\performance
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\msasn1
  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\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\imagehlp.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll
  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\cryptui.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\riched20.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shdocvw.dll
  Opens key:                HKCU\software\classes\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
  Opens key:                HKCR\clsid\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}
  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\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
  Opens key:                HKCU\software\microsoft\windows\shellnoroam\bags\22\shell
  Opens key:                HKCU\software\classes\directory\shellex\category
  Opens key:                HKCR\directory\shellex\category
  Opens key:                HKCU\software\microsoft\windows\shell
  Opens key:                HKCU\software\microsoft\windows\shell\localizedresourcename
  Opens key:                HKCU\software\classes\drive\shellex\folderextensions
  Opens key:                HKCR\drive\shellex\folderextensions
  Opens key:                HKCU\software\classes\drive\shellex\folderextensions\{fbeb8a05-beee-
4442-804e-409d6c4515e9}
  Opens key:                HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\cabinetstate
  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[1e582d1e5a53441b694d7073a8bbc09c]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[1e582d1e5a53441b694d7073a8bbc09c]
  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:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:            HKCU\control panel\desktop[lamebuttontext]
  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:            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\software\microsoft\ctf[disable thread input manager]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
  Queries value:            HKLM\software\microsoft\windows\currentversion\explorer[max cached
icons]
  Queries value:            HKCU\control panel\desktop\windowmetrics[shell icon size]
  Queries value:            HKCU\control panel\desktop\windowmetrics[shell small icon size]
  Queries value:            HKCU\control panel\desktop\windowmetrics[shell icon bpp]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline
files[suppressionpolicy]
  Queries value:
HKLM\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\offline
files[]
  Queries value:            HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}\inprocserver32[]
  Queries value:            HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32[loadwithoutcom]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager\appcompatibility[disableappcompat]
  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\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-080036587f03}[appid]
  Queries value:            HKCR\clsid\{750fdf0e-2a26-11d1-a3ea-
080036587f03}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[dontshowsuperhidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
```

```
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
  Queries value:               HKCR\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}\inprocserver32[]
  Queries value:               HKCR\clsid\{603d3800-bd81-11d0-a3a5-00c04fd706ec}[appid]
  Queries value:               HKCR\clsid\{603d3800-bd81-11d0-a3a5-
00c04fd706ec}\inprocserver32[threadingmodel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nonethood]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmycomputer]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nointerneticon]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocommongroups]
  Queries value:               HKLM\system\currentcontrolset\control\session
manager[safeprocesssearchmode]
  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\rpc[maxrpcsize]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[data]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-
11e3-9fc7-806d6172696f}[generation]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autocomplete in file dialog]
  Queries value:               HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}\inprocserver32[]
  Queries value:               HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[loadwithoutcom]
  Queries value:               HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{03c036f1-a186-11d0-824a-00aa005b4383}[appid]
  Queries value:               HKCR\clsid\{03c036f1-a186-11d0-824a-
00aa005b4383}\inprocserver32[threadingmodel]
  Queries value:               HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}\inprocserver32[]
  Queries value:               HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[loadwithoutcom]
  Queries value:               HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[inprocserver32]
  Queries value:               HKCR\clsid\{00bb2763-6a77-11d0-a535-00c04fd7d062}[appid]
  Queries value:               HKCR\clsid\{00bb2763-6a77-11d0-a535-
00c04fd7d062}\inprocserver32[threadingmodel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[alwaysdropup]
  Queries value:               HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[use
autocomplete]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[append completion]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[autosuggest]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\autocomplete[always use tab]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
  Queries value:
```

```
HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cd burning]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[userenvdebuglevel]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[chkaccdebuglevel]
  Queries value:            HKLM\system\currentcontrolset\control\productoptions[producttype]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local settings]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\winlogon[rsopdebuglevel]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\winlogon[rsoplogging]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileimagepath]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru[mrulist]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\comdlg32\lastvisitedmru[a]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[noviewondrive]
  Queries value:            HKCR\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[attributes]
  Queries value:            HKCR\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[callforattributes]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nocontrolpanel]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nosetfolders]
  Queries value:            HKCR\clsid\{20d04fe0-3aea-1069-a2d8-08002b30309d}\inprocserver32[]
  Queries value:            HKCR\directory[docobject]
  Queries value:            HKCR\directory[browseinplace]
  Queries value:            HKCR\directory[isshortcut]
  Queries value:            HKCR\directory[alwaysshowext]
  Queries value:            HKCR\directory[nevershowext]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinicache]
  Queries value:            HKCR\network\sharinghandler[]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nopropertiesmydocuments]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\nonenum[{450d8fba-ad25-11d0-98a8-
0800361b1103}]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\defaulticon[]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}\defaulticon[openicon]
  Queries value:            HKCR\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[wantsfordisplay]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\clsid\{450d8fba-
ad25-11d0-98a8-0800361b1103}[]
  Queries value:            HKCR\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[hidefolderverbs]
  Queries value:            HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}[localizedstring]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[flags]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[state]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[userpreference]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[centralprofile]
```

```
  Queries value:         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimelow]
  Queries value:         HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003[profileloadtimehigh]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\muicache[langid]
  Queries value:
HKCU\software\microsoft\windows\shellnoroam\muicache[@c:\windows\system32\shell32.dll,-9227]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
  Queries value:         HKCR\clsid\{450d8fba-ad25-11d0-98a8-
0800361b1103}\shellfolder[wantsforparsing]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my pictures]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my video]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[classicviewstate]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer[iconunderline]
  Queries value:         HKLM\software\microsoft\windows\currentversion\explorer[iconunderline]
  Queries value:         HKCU\software\microsoft\internet explorer\main[anchor underline]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
  Queries value:         HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common start menu]
  Queries value:         HKCR\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\inprocserver32[inprocserver32]
  Queries value:         HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}\inprocserver32[]
  Queries value:         HKCR\clsid\{42aedc87-2188-41fd-b9a3-0c966feabec1}[appid]
  Queries value:         HKCR\clsid\{42aedc87-2188-41fd-b9a3-
0c966feabec1}\inprocserver32[threadingmodel]
  Queries value:         HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
  Queries value:         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[1e582d1e5a53441b694d7073a8bbc09c.exe]
  Queries value:         HKLM\software\microsoft\internet
explorer\main\featurecontrol\feature_protocol_lockdown[*]
  Queries value:         HKLM\system\currentcontrolset\control\wmi\security[df8480a1-7492-4f45-
ab78-1084642581fb]
  Queries value:         HKLM\system\currentcontrolset\control\wmi\security[00000000-0000-0000-
0000-000000000000]
  Queries value:         HKLM\system\currentcontrolset\services\ldap[ldapclientintegrity]
  Queries value:         HKCR\interface\{eab22ac1-30c1-11cf-a7eb-0000c05bae0b}\typelib[]
  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[]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam[bagmru size]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bagmru[mrulistex]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bagmru[nodeslots]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bagmru[0]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bagmru[3]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bagmru\3[mrulistex]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bagmru\3[nodeslot]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\bags\22\shell[foldertype]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[sortmaxitemcount]
  Queries value:
HKCU\software\microsoft\windows\shell\localizedresourcename[@shell32.dll,-21779]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\muicache[@shell32.dll,-
21779]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my music]
  Queries value:
HKCU\software\microsoft\windows\shell\localizedresourcename[@shell32.dll,-21790]
  Queries value:         HKCU\software\microsoft\windows\shellnoroam\muicache[@shell32.dll,-
21790]
  Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[nostrcmplogical]
  Queries value:         HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
  Queries value:         HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
```

```
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\cabinetstate[settings]
   Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\cabinetstate[fullpath]
   Queries value:
HKCU\software\microsoft\windows\currentversion\policies\explorer[comparejunctionness]
   Sets/Creates value:           HKCU\software\microsoft\windows\shellnoroam\muicache[@shell32.dll,-
21779]
   Sets/Creates value:           HKCU\software\microsoft\windows\shellnoroam\muicache[@shell32.dll,-
21790]
   Value changes:                HKLM\software\microsoft\cryptography\rng[seed]
   Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}[baseclass]
   Value changes:                HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
   Value changes:                HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[recent]
   Value changes:                HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
   Value changes:                HKCU\software\microsoft\windows\shellnoroam\bagmru[nodeslots]
   Value changes:                HKCU\software\microsoft\windows\shellnoroam\bagmru[mrulistex]
   Value changes:                HKCU\software\microsoft\windows\shellnoroam\bags\22\shell[foldertype]
   Value changes:                HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[favorites]
```