

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 60, Task ID: 239

Task ID:	239
Risk Level:	5
Date Processed:	2016-04-28 12:53:54 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe"
Sample ID:	60
Type:	basic
Owner:	admin
Label:	3967487e5d2dae5d459d7d491277238c
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	368304 bytes
MD5:	3967487e5d2dae5d459d7d491277238c
SHA256:	f91da84d3f4708c5323fa0ed783ecb6f2e66993db47dadff993c637f5c2a5cd7
Description:	None

Pattern Matching Results

2	PE: Nonstandard section
5	Packer: UPX
5	PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\3967487e5d2dae5d459d7d491277238c.exe
["c:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe"]	

Named Object Events

Creates mutex:	\BaseNamedObjects\3967487e5d2dae5d459d7d491277238c.exeesoc19uK
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-
507921405-1957994488-1003	MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}
Creates semaphore:	\BaseNamedObjects\INI-3967487e5d2dae5d459d7d491277238c.data
Creates semaphore:	\BaseNamedObjects\GR_FileChecker
Creates semaphore:	\BaseNamedObjects\GR0
Creates semaphore:	\BaseNamedObjects\GR_FlushingList
Creates semaphore:	\BaseNamedObjects\GR_Write
Creates semaphore:	\BaseNamedObjects\GR_GErrMsg
Creates semaphore:	\BaseNamedObjects\GR1
Creates semaphore:	\BaseNamedObjects\GR2
Creates semaphore:	\BaseNamedObjects\GR3
Creates semaphore:	\BaseNamedObjects\GR4
Creates semaphore:	\BaseNamedObjects\GR5
Creates semaphore:	\BaseNamedObjects\GR6
Creates semaphore:	\BaseNamedObjects\GR7
Creates semaphore:	\BaseNamedObjects\GR8
Creates semaphore:	\BaseNamedObjects\GR9
Creates semaphore:	\BaseNamedObjects\GR10
Creates semaphore:	\BaseNamedObjects\GR11
Creates semaphore:	\BaseNamedObjects\GR12
Creates semaphore:	\BaseNamedObjects\GR13
Creates semaphore:	\BaseNamedObjects\GR14
Creates semaphore:	\BaseNamedObjects\GR15
Creates semaphore:	\BaseNamedObjects\GR16
Creates semaphore:	\BaseNamedObjects\GR17
Creates semaphore:	\BaseNamedObjects\GR18
Creates semaphore:	\BaseNamedObjects\GR19
Creates semaphore:	\BaseNamedObjects\GR20

[illegible]

File System Events

Creates: C:\Documents and Settings
Creates: C:\Documents and Settings\Admin
Creates: C:\Documents and Settings\Admin\Application Data
Creates: C:\Documents and Settings\Admin\Application Data\GetRightToGo
Creates: C:\Documents and Settings\Admin\Application Data\GetRightToGo\
Creates: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
Creates: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
Opens: C:\WINDOWS\Prefetch\3967487E5D2DAE5D459D7D4912772-2A8E1203.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\oledlg.dll
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.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\temp\3967487e5d2dae5d459d7d491277238c.exe.2.Manifest
Opens: C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.3.Manifest
Opens: C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.Manifest
Opens: C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.Config
Opens: C:\windows\temp\3967487e5d2dae5d459d7d491277238c.exe.1000.Manifest
Opens: C:\
Opens: C:\Documents and Settings\Admin\Local Settings
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\setupapi.dll
Opens: C:\Documents and Settings
Opens: C:\Documents and Settings\All Users
Opens: C:\Documents and Settings\Admin\Application Data\desktop.ini
Opens: C:\Documents and Settings\Admin\Application Data\GetRightToGo
Opens: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
Opens: C:\WINDOWS\Temp
Opens: C:\WINDOWS\Temp\3967487e5d2dae5d459d7d491277238c.exe
Opens: C:\WINDOWS\Temp\163df993-80c0-448a-9917-78c69a8e6968
Opens: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
Opens: C:\Documents and Settings\All Users\Desktop
Opens: C:\Documents and Settings\Admin\Desktop\Downloads\
Opens: C:\WINDOWS\Fonts\sserife.fon
Writes to: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
Writes to: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0
Reads from: C:\Documents and Settings\Admin\Application Data\desktop.ini
Reads from: C:\WINDOWS\Temp\3967487e5d2dae5d459d7d491277238c.exe
Reads from: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data
Reads from: C:\Documents and Settings\Admin\Application
Data\GetRightToGo\3967487e5d2dae5d459d7d491277238c.data0

Windows Registry Events

Creates key: HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
Creates key: HKLM\software\microsoft\windows\currentversion\explorer\shell folders
Creates key:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-
806d6172696f}\
Creates key: HKCU\software\headlight
Creates key: HKCU\software\headlight\getrighttogo
Creates key: HKCU\software\headlight\getrighttogo\sharedconfig
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
Creates key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
Creates key: HKCU\software\headlight\getrighttogo\customizedapps
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\3967487e5d2dae5d459d7d491277238c.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\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oledlg.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\winspool.drv	
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\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\ole
Opens key:	HKCR\interface
Opens key:	HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\oleaut\userera
Opens key:	HKCU\software\classes\
Opens key:	HKCU\software\classes\clsid
Opens key:	HKCR\clsid
Opens key:	HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key:	HKCU\software\microsoft\windows\currentversion\policies\network
Opens key:	HKCU\software\microsoft\windows\currentversion\policies\comdlg32
Opens key:	HKLM\system\currentcontrolset\control\computername
Opens key:	HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll	
Opens key:	
HKLM\software\microsoft\ctf\compatibility\3967487e5d2dae5d459d7d491277238c.exe	
Opens key:	HKLM\software\microsoft\ctf\systemshared\
Opens key:	HKCU\keyboard layout\toggle
Opens key:	HKLM\software\microsoft\ctf\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\imm
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll	
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution

```

options\msctfime.ime
  Opens key: HKCU\software\microsoft\ctf
  Opens key: HKLM\software\microsoft\ctf\systemshared
  Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\uxtheme.dll
  Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
  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\currentversion\policies\explorer
  Opens key: HKLM\software\microsoft\windows\currentversion\shellcompatibility\applications\3967487e5d2dae5d459d7d491277238c.exe
  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: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\setupapi.dll
  Opens key: HKLM\system\currentcontrolset\control\minint
  Opens key: HKLM\system\wpa\pnf
  Opens key: HKLM\software\microsoft\windows\currentversion\setup
  Opens key: HKLM\software\microsoft\windows\currentversion
  Opens key: HKLM\software\microsoft\windows\currentversion\setup\apploglevels
  Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters
  Opens key: HKLM\software\policies\microsoft\system\dnscient
  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\3967487e5d2dae5d459d7d491277238c.exe\rpcthreadpoolthrottle
  Opens key: HKLM\software\policies\microsoft\windows nt\rpc
  Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume
  Opens key: HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\cpc\volume\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
  Opens key: HKCU\software\classes\directory
  Opens key: HKCR\directory
  Opens key: HKCU\software\classes\directory\curver
  Opens key: HKCR\directory\curver
  Opens key: HKCR\directory\
  Opens key: HKCU\software\microsoft\windows\currentversion\explorer
  Opens key: HKCU\software\microsoft\windows\currentversion\explorer\
  Opens key: HKCU\software\microsoft\windows\currentversion\policies\system

```

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
 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\{450d8fba-ad25-11d0-98a8-0800361b1103}
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\nonenum
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\nonenum
 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
 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[3967487e5d2dae5d459d7d491277238c]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\imecompatibility[3967487e5d2dae5d459d7d491277238c]
 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: 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\windows\currentversion\policies\explorer[norun]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
 Queries value:
 HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
 Queries value: HKCU\keyboard layout\toggle[language hotkey]
 Queries value: HKCU\keyboard layout\toggle[hotkey]
 Queries value: HKCU\keyboard layout\toggle[layout hotkey]
 Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
 Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
 Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
 Queries value: HKCU\control panel\desktop[lamebuttontext]
 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]

[illegible]

folders[common desktop]
 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: HKLM\system\wpa\pnp[seed]
 Queries value: HKLM\system\setup[osloaderpath]
 Queries value: HKLM\system\setup[systempartition]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value:
 HKLM\software\microsoft\windows\currentversion\setup[servicepacksourcepath]
 Queries value:
 HKLM\software\microsoft\windows\currentversion\setup[servicepackcachepath]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[drivercachepath]
 Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[loglevel]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[logpath]
 Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname]
 Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]
 Queries value: HKLM\software\microsoft\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\policies\explorer[dontshowsuperhidden]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer[shellstate]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[forceactivedesktopon]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[noactivedesktop]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nowebview]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[classicshell]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[separateprocess]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetcrawling]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[nosimplestartmenu]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidden]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[showcompcolor]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[hidefileext]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[dontprettypath]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[showinfotip]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[hideicons]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[mapnetdrvbtn]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[webview]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[filter]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[showsuperhidden]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[separateprocess]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\explorer\advanced[nonetcrawling]
 Queries value: HKCR\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\headlight\getrighttogo\sharedconfig[useloadimage]
 Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[doxpthemes]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[appdata]
 Queries value:
 HKCU\software\microsoft\windows\currentversion\policies\explorer[usedesktopinocache]
 Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[debug]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
 folders[desktop]
 Queries value: HKCU\software\headlight\getrighttogo\sharedconfig[screenreader]
 Queries value: HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[wantsforparsing]

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[personal]
Queries value: HKCR\clsid\{450d8fba-ad25-11d0-98a8-0800361b1103}\shellfolder[attributes]
Queries value: HKLM\software\microsoft\windows\currentversion\policies\nonenum[{450d8fba-ad25-11d0-98a8-0800361b1103}]
Sets/Creates value: HKCU\software\headlight\getrighttogo\customizedapps[3967487e5d2dae5d459d7d491277238c]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[busypause]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecache]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[filecachekb]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[rollback]
Sets/Creates value: HKCU\software\headlight\getrighttogo\sharedconfig[dotgetright]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes: HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common desktop]
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[appdata]
Value changes: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]