Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	695
Risk Level:	5
Date Processed:	2016-04-28 13:06:31 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\c15f543da83b0ca8766e750f61a8b0f7.exe"
Sample ID:	174
Type:	basic
Owner:	admin
Label:	c15f543da83b0ca8766e750f61a8b0f7
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	692224 bytes
MD5:	c15f543da83b0ca8766e750f61a8b0f7
SHA256:	e40bf835e832252ce631ad2da6fe179d3bca874503496541ca7dda21e894371d
Description:	None

Pattern Matching Results

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

Static Events

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

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\c15f543da83b0ca8766e750f61a8b0f7.exe ["c:\windows\temp\c15f543da83b0ca8766e750f61a8b0f7.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\MutexNPA_UnitVersioning_1300
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.MK
Creates event:	\BaseNamedObjects\userenv: User Profile setup event
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{210A4BA0-3AEA-1069-A2D9-08002B30309D}

File System Events

Opens:	C:\WINDOWS\Prefetch\C15F543DA83B0CA8766E750F61A8B-001FFFE2.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\hhctrl.ocx
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\wsock32.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\Temp\c15f543da83b0ca8766e750f61a8b0f7.exe
Opens:	C:\
Opens:	C:\WINDOWS\system32\MSCTF.dll

```
  Opens:                 C:\WINDOWS\system32\MSCTFIME.IME
  Opens:                 C:\WINDOWS\system32\wship6.dll
  Opens:                 C:\WINDOWS\system32\rpcss.dll
  Opens:                 C:\WINDOWS\system32\uxtheme.dll
  Opens:                 C:\WINDOWS\Fonts\sserife.fon
```

Windows Registry Events

```
  Creates key:           HKCR\.key
  Creates key:           HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:           HKCU\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:           HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders
  Creates key:           HKLM\software\microsoft\windows\currentversion\explorer\shell folders
  Creates key:           HKCU\software\recovery toolbox for rar
  Creates key:           HKCU\software\recovery toolbox for rar\cbfilename
  Creates key:           HKCU\software\recovery toolbox for rar\cbunzipfolder
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\c15f543da83b0ca8766e750f61a8b0f7.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\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\msvcrt.dll
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\software\microsoft\windows nt\currentversion\image file execution
options\hhctrl.ocx
  Opens key:             HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:             HKLM\system\currentcontrolset\control\error message instrument
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:             HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:             HKLM\software\microsoft\ole
  Opens key:             HKCR\interface
  Opens key:             HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:             HKLM\software\microsoft\oleaut
  Opens key:             HKLM\software\microsoft\oleaut\userera
  Opens key:             HKCU\
  Opens key:             HKCU\software\policies\microsoft\control panel\desktop
  Opens key:             HKCU\control panel\desktop
  Opens key:             HKLM\software\microsoft\windows\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\rpc\pagedbuffers
  Opens key:                HKLM\software\microsoft\rpc
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\c15f543da83b0ca8766e750f61a8b0f7.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 nt\currentversion\image file execution
options\ws2help.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ws2_32.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wsock32.dll
  Opens key:                HKCU\software\borland\locales
  Opens key:                HKCU\software\borland\delphi\locales
  Opens key:                HKLM\system\currentcontrolset\services\winsock2\parameters
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000003
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000006
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000007
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000009
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\00000004
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002
  Opens key:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003
  Opens key:                HKCU\software\recovery toolbox for rar
  Opens key:                HKLM\software\recovery toolbox for rar
  Opens key:                HKCU\software\classes\
  Opens key:                HKCU\software\classes\.key
  Opens key:                HKLM\software\classes
  Opens key:                HKCR\.key
  Opens key:                HKLM\software\borland\locales
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\c15f543da83b0ca8766e750f61a8b0f7.exe
  Opens key:                HKLM\software\microsoft\ctf\systemshared\
  Opens key:                HKCU\keyboard layout\toggle
  Opens key:                HKLM\software\microsoft\ctf\
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\imm
  Opens key:                HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctfime.ime
  Opens key:                HKCU\software\microsoft\ctf
  Opens key:                HKLM\software\microsoft\ctf\systemshared
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wship6.dll
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\image file execution
options\userenv.dll
  Opens key:                HKLM\system\currentcontrolset\control\productoptions
  Opens key:                HKCU\software\microsoft\windows\currentversion\explorer\user shell
```

```
folders
  Opens key:                HKLM\software\policies\microsoft\windows\system
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist\s-1-5-21-
1757981266-507921405-1957994488-1003
  Opens key:                HKLM\software\microsoft\windows nt\currentversion\profilelist
  Opens key:                HKLM\software\microsoft\windows\currentversion
  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\microsoft\ctf\langbaraddin\
  Opens key:                HKLM\software\microsoft\ctf\langbaraddin\
  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[c15f543da83b0ca8766e750f61a8b0f7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[c15f543da83b0ca8766e750f61a8b0f7]
  Queries value:            HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:            HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:            HKCR\interface[interfacehelperdisableall]
  Queries value:            HKCR\interface[interfacehelperdisableallforole32]
  Queries value:            HKCR\interface[interfacehelperdisabletypelib]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:            HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:            HKCU\control panel\desktop[multiuilanguageid]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  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\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\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
  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\explorer\user shell
folders[administrative tools]
  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\user shell
folders[altstartup]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[appdata]
  Queries value:            HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cd burning]
  Queries value:            HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common administrative tools]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[profilesdirectory]
  Queries value:            HKLM\software\microsoft\windows
nt\currentversion\profilelist[allusersprofile]
```

```
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common altstartup]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common appdata]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common desktop]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common documents]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common favorites]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonmusic]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonpictures]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common programs]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common start menu]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common startup]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[common templates]
  Queries value:             HKLM\software\microsoft\windows\currentversion\explorer\user shell
folders[commonvideo]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cookies]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[desktop]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[favorites]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[fonts]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[history]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[cache]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[local appdata]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[my music]
  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[nethood]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[printhood]
  Queries value:             HKLM\software\microsoft\windows\currentversion[programfilesdir]
  Queries value:             HKLM\software\microsoft\windows\currentversion[commonfilesdir]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[programs]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[recent]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[sendto]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[start menu]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[startup]
  Queries value:             HKCU\software\microsoft\windows\currentversion\explorer\user shell
folders[templates]
  Queries value:             HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
  Queries value:             HKCU\control panel\desktop[lamebuttontext]
  Queries value:             HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
sans serif]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\fontsubstitutes[tahoma]
  Queries value:             HKCU\software\recovery toolbox for rar[installpath]
  Queries value:             HKCU\software\recovery toolbox for rar\cbfilename[val0]
  Queries value:             HKCU\software\recovery toolbox for rar\cbunzipfolder[val0]
  Sets/Creates value:        HKCR\.key[]
  Value changes:             HKLM\software\microsoft\cryptography\rng[seed]
  Value changes:             HKCR\.key[]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[administrative tools]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[appdata]
  Value changes:             HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cd
burning]
  Value changes:             HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common administrative tools]
  Value changes:             HKLM\software\microsoft\windows\currentversion\explorer\shell
```

```
folders[common appdata]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common desktop]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common documents]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common favorites]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[commonmusic]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[commonpictures]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common programs]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common start menu]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common startup]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[common templates]
  Value changes:           HKLM\software\microsoft\windows\currentversion\explorer\shell
folders[commonvideo]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cookies]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[favorites]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[fonts]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[history]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[cache]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[local appdata]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
music]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
pictures]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell folders[my
video]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[nethood]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[personal]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[printhood]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[programs]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[recent]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[sendto]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[start menu]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[startup]
  Value changes:           HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[templates]
```