Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	899
Risk Level:	4
Date Processed:	2016-04-28 13:12:20 (UTC)
Processing Time:	2.61 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe"
Sample ID:	225
Type:	basic
Owner:	admin
Label:	6d438b3e1ec4eca849107b093ce99dbc
Date Added:	2016-04-28 12:45:13 (UTC)
File Type:	PE32:win32:gui
File Size:	927416 bytes
MD5:	6d438b3e1ec4eca849107b093ce99dbc
SHA256:	9977dc742345ebc75d8914773e0af884e6ee16227f7acf9361fff7b681b971fc
Description:	None

Pattern Matching Results

`2` PE: Nonstandard section
`4` Packer: NSIS [Nullsoft Scriptable Install System]

Static Events

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

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe

["c:\windows\temp\6d438b3e1ec4eca849107b093ce99dbc.exe"]

Terminates process:	C:\WINDOWS\Temp\6d438b3e1ec4eca849107b093ce99dbc.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 semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Creates semaphore:	\BaseNamedObjects\shell.{7CB834F0-527B-11D2-9D1F-0000F805CA57}

File System Events

Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw1.tmp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp
Creates:	C:\DOCUME~1
Creates:	C:\DOCUME~1\Admin
Creates:	C:\DOCUME~1\Admin\LOCALS~1

Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp
Creates:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp\System.dll
Creates:	C:\DOCUME~1\Admin\LOCALS~1\Temp\nsd2.tmp\System.dll
Opens:	C:\WINDOWS\Prefetch\6D438B3E1EC4ECA849107B093CE99-2B6D682A.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\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\shfolder.dll
Opens:	C:\WINDOWS\system32\setupapi.dll
Opens:	C:\
Opens:	C:\Documents and Settings
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw1.tmp
Opens:	C:\WINDOWS\Temp\d06a48e3-c243-4b43-a571-1b5c5e42a50a
Opens:	C:\WINDOWS\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp
Opens:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp\System.dll
Opens:	C:\windows\temp\distribution\
Opens:	C:\WINDOWS\Temp
Opens:	C:\WINDOWS
Opens:	C:\Documents and Settings\Admin\Local Settings
Writes to:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp\System.dll
Reads from:	C:\WINDOWS\Temp\6d438b3e1ec4eca849107b093ce99dbc.exe
Deletes:	C:\Documents and Settings\Admin\Local Settings\Temp\nsw1.tmp
Deletes:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp
Deletes:	C:\Documents and Settings\Admin\Local Settings\Temp\nsd2.tmp\System.dll

Windows Registry Events

Creates key:	HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\6d438b3e1ec4eca849107b093ce99dbc.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\gdi32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\user32.dll
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\imm32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\kernel32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\secur32.dll
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution

```
options\rpcrt4.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\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\comctl32.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\version.dll
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument\
  Opens key:              HKLM\system\currentcontrolset\control\error message instrument
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\gre_initialize
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\compatibility32
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\ime compatibility
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\windows
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\winlogon
  Opens key:              HKLM\
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\diagnostics
  Opens key:              HKLM\software\microsoft\windows\currentversion\explorer\performance
  Opens key:              HKLM\system\setup
  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\software\microsoft\ole
  Opens key:              HKCR\interface
  Opens key:              HKCR\interface\{00020400-0000-0000-c000-000000000046}
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
  Opens key:
HKLM\software\microsoft\ctf\compatibility\6d438b3e1ec4eca849107b093ce99dbc.exe
  Opens key:              HKLM\software\microsoft\ctf\systemshared\
  Opens key:              HKCU\keyboard layout\toggle
  Opens key:              HKLM\software\microsoft\ctf\
  Opens key:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shfolder.dll
  Opens key:              HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:              HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:
HKLM\software\microsoft\windows\currentversion\shellcompatibility\objects\{20d04fe0-3aea-1069-
a2d8-08002b30309d}
  Opens key:              HKCU\software\classes\
  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\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\6d438b3e1ec4eca849107b093ce99dbc.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\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\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:              HKLM\software\microsoft\windows nt\currentversion\image file execution
options\system.dll
  Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
  Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value:          HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:          HKLM\software\microsoft\windows
nt\currentversion\compatibility32[6d438b3e1ec4eca849107b093ce99dbc]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[6d438b3e1ec4eca849107b093ce99dbc]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
  Queries value:          HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
  Queries value:          HKLM\system\setup[systemsetupinprogress]
  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\currentcontrolset\control\session
manager[criticalsectiontimeout]
  Queries value:          HKLM\software\microsoft\ole[rwlockresourcetimeout]
  Queries value:          HKCR\interface[interfacehelperdisableall]
  Queries value:          HKCR\interface[interfacehelperdisableallforole32]
  Queries value:          HKCR\interface[interfacehelperdisabletypelib]
  Queries value:          HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
  Queries value:          HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
  Queries value:          HKLM\software\microsoft\ctf\systemshared[cuas]
  Queries value:          HKCU\keyboard layout\toggle[language hotkey]
```

```
Queries value:              HKCU\keyboard layout\toggle[hotkey]
Queries value:              HKCU\keyboard layout\toggle[layout hotkey]
Queries value:              HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value:
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:
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\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:              HKCR\drive\shellex\folderextensions\{fbeb8a05-beee-4442-804e-
409d6c4515e9}[drivemask]
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: HKLM\software\microsoft\windows\currentversion[programfilesdir]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]
Value changes:
HKCU\software\microsoft\windows\currentversion\explorer\mountpoints2\{f90255c2-6bc4-11e3-9fc7-806d6172696f}[baseclass]