Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	190
Risk Level:	1
Date Processed:	2016-04-28 12:52:22 (UTC)
Processing Time:	62.49 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.exe"
Sample ID:	48
Type:	basic
Owner:	admin
Label:	9d240291c8dc756bfafe75a7e60099cc
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	321536 bytes
MD5:	9d240291c8dc756bfafe75a7e60099cc
SHA256:	7c7b5307cc803bb037226eee0eca8b0a6f1d79d3d9d96755b29208442847466a
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\9d240291c8dc756bfafe75a7e60099cc.exe

["c:\windows\temp\9d240291c8dc756bfafe75a7e60099cc.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\MSCTF.Shared.MUTEX.EOG
Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens:	C:\WINDOWS\Prefetch\9D240291C8DC756BFAFE75A7E6009-32B4083A.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\wsock32.dll
Opens:	C:\WINDOWS\system32\ws2_32.dll
Opens:	C:\WINDOWS\system32\ws2help.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\shell32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\shell32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\Fonts\sserife.fon
Opens:	C:\windows\temp\updatewizard.ini
Opens:	C:\WINDOWS\system32\MSIMTF.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\9d240291c8dc756bfafe75a7e60099cc.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\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\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\comctl32.dll
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:          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\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\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:          HKCU\software\borland\delphi\locales
Opens key:          HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll
Opens key:
HKLM\software\microsoft\ctf\compatibility\9d240291c8dc756bfafe75a7e60099cc.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\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\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\session manager[safedllsearchmode]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
    Queries value: HKLM\software\microsoft\windows
nt\currentversion\compatibility32[9d240291c8dc756bfafe75a7e60099cc]
    Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[9d240291c8dc756bfafe75a7e60099cc]
    Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
    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[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\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:
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]
   Value changes: HKLM\software\microsoft\cryptography\rng[seed]