Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 77, Task ID: 307

Task ID:	307
Risk Level:	4
Date Processed:	2016-04-28 12:55:39 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe"
Sample ID:	77
Type:	basic
Owner:	admin
Label:	ca293fc948db9309896d46f093b9ca26
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	103008 bytes
MD5:	ca293fc948db9309896d46f093b9ca26
SHA256:	71d9958e04ef992e1b465094a4009364328284b5f81488c5c6dc0d24d216dc60
Description:	None

Pattern Matching Results

4 Reads process memory

Process/Thread Events

Creates process: C:\WINDOWS\Temp\ca293fc948db9309896d46f093b9ca26.exe ["c:\windows\temp\ca293fc948db9309896d46f093b9ca26.exe"]
Reads from process: PID:4 System
Reads from process: PID:388 C:\WINDOWS\system32\smss.exe
Reads from process: PID:668 C:\WINDOWS\system32\winlogon.exe
Reads from process: PID:896 C:\WINDOWS\system32\services.exe
Reads from process: PID:908 C:\WINDOWS\system32\lsass.exe
Reads from process: PID:1068 C:\WINDOWS\system32\svchost.exe
Reads from process: PID:1272 C:\WINDOWS\system32\svchost.exe
Reads from process: PID:1712 C:\WINDOWS\system32\spoolsv.exe
Reads from process: PID:1836 C:\WINDOWS\explorer.exe
Reads from process: PID:1896 C:\Program Files\Adobe\Reader 9.0\Reader\reader_sl.exe
Reads from process: PID:1912 C:\WINDOWS\system32\ctfmon.exe
Reads from process: PID:2028 C:\WINDOWS\system32\rundll32.exe
Reads from process: PID:260 C:\Program Files\Java\jre7\bin\jqs.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.AEH
Creates mutex: \BaseNamedObjects\MSCTF.Shared.MUTEX.EPF
Creates event: \BaseNamedObjects\MSCTF.SendReceive.Event.EPF.IC
Creates event: \BaseNamedObjects\MSCTF.SendReceiveConection.Event.EPF.IC
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Opens: C:\WINDOWS\Prefetch\CA293FC948DB9309896D46F093B9C-089CF1FA.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\system32\imm32.dll
Opens: C:\WINDOWS\WindowsShell.Manifest
Opens: C:\WINDOWS\WindowsShell.Config
Opens: C:\WINDOWS\system32\shell32.dll
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens: C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\system32\ole32.dll
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\windows\temp\ca293fc948db9309896d46f093b9ca26.cfg
Opens: C:\WINDOWS\system32\MSIMTF.dll
Opens: C:\WINDOWS\Fonts\arialbd.ttf
Opens: C:\WINDOWS\system32\mnmdd.dll
Opens: C:\WINDOWS\system32\rdpdd.dll
Opens: C:\WINDOWS\system32\psapi.dll
Opens: C:\WINDOWS\explorer.exe
Opens: C:\WINDOWS\system32\calc.exe
Reads from: C:\WINDOWS\explorer.exe

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ca293fc948db9309896d46f093b9ca26.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\msvcrt.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\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\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\version.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\shell32.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\comdlg32.dll
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key: HKLM\system\setup
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\ca293fc948db9309896d46f093b9ca26.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: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ole32.dll
Opens key: HKLM\software\microsoft\ole
Opens key: HKCR\interface
Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key: HKCU\software\microsoft\ctf
Opens key: HKLM\software\microsoft\ctf\systemshared
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\uxtheme.dll
Opens key: HKCU\software\microsoft\windows\currentversion\thememanager
Opens key: HKLM\software\microsoft\windows\currentversion\explorer\advanced
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKCU\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\software\microsoft\ctf\langbaraddin\
Opens key: HKLM\hardware\devicemap\video
Opens key: HKLM\system\currentcontrolset\hardware profiles\current\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000
Opens key: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000
Opens key: HKLM\system\currentcontrolset\hardware profiles\current\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000
Opens key: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000
Opens key: HKLM\system\currentcontrolset\control\watchdog\display
Opens key: HKLM\system\currentcontrolset\hardware profiles\current\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000
Opens key: HKLM\system\currentcontrolset\hardware

profiles\0001\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000
Opens key: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\psapi.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\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[ca293fc948db9309896d46f093b9ca26]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[ca293fc948db9309896d46f093b9ca26]
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\software\microsoft\ctf\systemshared[cuas]
Queries value: HKCU\keyboard layout\toggle[language hotkey]
Queries value: HKCU\keyboard layout\toggle[hotkey]
Queries value: HKCU\keyboard layout\toggle[layout hotkey]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
Queries value: HKLM\system\currentcontrolset\control\session manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-000000000046}[interfacehelperdisableallforole32]
Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
Queries value: HKCU\software\microsoft\windows\currentversion\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
Queries value: HKLM\software\microsoft\windows\currentversion\explorer\advanced[listviewscrollover]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewwatermark]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKLM\hardware\devicemap\video[maxobjectnumber]
Queries value: HKLM\hardware\devicemap\video[\device\video0]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.bitsperpel]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-

9b1f4867732a}\0000[defaultsettings.xresolution]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.yresolution]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.vrefresh]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.flags]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.xpanning]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.ypanning]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.orientation]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.fixedoutput]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[attach.relativex]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[attach.relativey]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[attach.todesktop]
Queries value: HKLM\system\currentcontrolset\hardware profiles\0001\system\currentcontrolset\control\video\{23a77bf7-ed96-40ec-af06-9b1f4867732a}\0000[defaultsettings.driverextra]
Queries value: HKLM\hardware\devicemap\video[\device\video1]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.bitsperpel]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.xresolution]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.yresolution]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.vrefresh]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.flags]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.xpanning]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.ypanning]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.orientation]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.fixedoutput]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[attach.relativex]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[attach.relativey]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[attach.todesktop]
Queries value: HKLM\system\currentcontrolset\control\video\{8b6d7859-a639-4a15-8790-7161976d057a}\0000[defaultsettings.driverextra]
Queries value: HKLM\system\currentcontrolset\control\watchdog\display[earecovery]
Queries value: HKLM\system\currentcontrolset\control\watchdog\display[fullrecovery]

Queries value: HKLM\hardware\devicemap\video[\device\video2]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.bitsperpel]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.xresolution]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.yresolution]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.vrefresh]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.flags]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.xpanning]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.ypanning]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.orientation]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.fixedoutput]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[attach.relativex]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[attach.relativey]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[attach.todesktop]
Queries value: HKLM\system\currentcontrolset\control\video\{deb039cc-b704-4f53-b43e-9dd4432fa2e9}\0000[defaultsettings.driverextra]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]