Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 134, Task ID: 535

Task ID:	535
Risk Level:	5
Date Processed:	2016-04-28 13:01:49 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\2a331c13d2c596ffd675768823c8930d.exe"
Sample ID:	134
Type:	basic
Owner:	admin
Label:	2a331c13d2c596ffd675768823c8930d
Date Added:	2016-04-28 12:45:04 (UTC)
File Type:	PE32:win32:gui
File Size:	896000 bytes
MD5:	2a331c13d2c596ffd675768823c8930d
SHA256:	0cc7c6045521da5ecf43219c120eda04ff5e7c8727659f863d3894dcf203b7b7
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\2a331c13d2c596ffd675768823c8930d.exe
["c:\windows\temp\2a331c13d2c596ffd675768823c8930d.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.IAB
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#0
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#1
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#2
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#3
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#4
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#5
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#6
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#7
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#8
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#9
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#10
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#11
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#12
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#13
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#14
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#15

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#16
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#17
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#18
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#19
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#20
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#21
Creates: C:\Documents and Settings\Admin\Local Settings\Temp\ic#22
Opens: C:\WINDOWS\Prefetch\2A331C13D2C596FFD675768823C89-29A7FC86.pf
Opens: C:\Documents and Settings\Admin
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\system32\msimg32.dll
Opens: C:\WINDOWS\system32\rpcss.dll
Opens: C:\WINDOWS\system32\uxtheme.dll
Opens: C:\WINDOWS\Fonts\arialbd.ttf
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#0
Opens: C:\WINDOWS\Temp\2ee67436-c159-48f4-8e40-0226ea6b6de3
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#1
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#2
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#3
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#4
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#5
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#6
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#7
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#8
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#9
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#10
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#11
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#12
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#13
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#14
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#15
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#16
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#17
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#18
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#19
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#20
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#21
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\ic#22
Opens: C:\WINDOWS\system32\MSIMTF.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#0
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#1
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#2
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#3
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#4
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#5
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#6
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#7
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#8
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#9
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#10
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#11
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#12
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#13
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#14
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#15
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#16
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#17
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#18
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#19

Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#20
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#21
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\ic#22
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#0
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#1
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#2
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#3
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#4
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#5
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#6
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#7
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#8
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#9
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#10
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#11
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#12
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#13
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#14
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#15
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#16
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#17
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#18
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#19
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#20
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#21
Reads from: C:\Documents and Settings\Admin\Local Settings\Temp\ic#22
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#0
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#1
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#2
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#3
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#4
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#5
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#6
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#7
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#8
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#9
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#10
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#11
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#12
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#13
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#14
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#15
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#16
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#17
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#18
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#19
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#20
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#21
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\ic#22

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\2a331c13d2c596ffd675768823c8930d.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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\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\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\comctl32.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\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\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: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
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: 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\locales
Opens key: HKLM\software\borland\locales
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\2a331c13d2c596ffd675768823c8930d.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\msimg32.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\applications\2a331c13d2c596ffd675768823c8930d.exe
Opens key: HKCU\software\exejoiner_dem
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 nt\currentversion\fontsubstitutes
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\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\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[2a331c13d2c596ffd675768823c8930d]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[2a331c13d2c596ffd675768823c8930d]
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: 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\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: 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\thememanager[compositing]
Queries value: HKCU\control panel\desktop[lamebuttontext]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\advanced[usedoubleclicktimer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]