Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 89, Task ID: 355

Task ID:	355
Risk Level:	8
Date Processed:	2016-04-28 12:56:49 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe"
Sample ID:	89
Type:	basic
Owner:	admin
Label:	906eb2c5b0eee128a609c1bae001562f
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	737280 bytes
MD5:	906eb2c5b0eee128a609c1bae001562f
SHA256:	b96667f35d996516559f9bbab7d295ca1ae2875b17ea2cfe74f200184d8577ba
Description:	None

Pattern Matching Results

3 PE: File has non-standard alignment
2 64 bit executable
4 Checks whether debugger is present
5 Resource section contains an executable
2 PE: Nonstandard section
8 Contains suspicious Microsoft certificate

Static Events

Anomaly:	PE: File has non-standard file alignment
Anomaly:	PE: File has non-standard section alignment
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: Resource section contains an executable

Process/Thread Events

Creates process: C:\WINDOWS\Temp\906eb2c5b0eee128a609c1bae001562f.exe ["c:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe"]
Loads service: cpuz129 [\??\C:\DOCUME~1\Admin\LOCALS~1\Temp\cpuz_x32.sys]

Named Object Events

Creates mutex: \BaseNamedObjects\CPUIDSDK
Creates mutex: \BaseNamedObjects\cpuz
Creates mutex: \BaseNamedObjects\PERFMON0
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.IDH
Creates semaphore: \BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}

File System Events

Creates: C:\Documents and Settings\Admin\Local Settings\Temp\cpuz_x32.sys
Opens: C:\WINDOWS\Prefetch\906EB2C5B0EEE128A609C1BAE0015-20D848BD.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winspool.drv
Opens: C:\WINDOWS\system32\winmm.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\temp\906eb2c5b0eee128a609c1bae001562f.exe.2.Manifest
Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.3.Manifest
Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.Manifest
Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.Config
Opens: C:\DOCUME~1\Admin\LOCALS~1\Temp\cpuz_x32.sys
Opens: C:\Documents and Settings\Admin\Local Settings\Temp
Opens: C:\Documents and Settings\Admin\Local Settings\Temp\cpuz_x32.sys
Opens: C:\WINDOWS\Temp\780b3e49-0776-484b-8326-2466299904b4
Opens: C:\WINDOWS\system32\powrprof.dll
Opens: C:PerfMonitor0.ini
Opens: C:\WINDOWS\system32\MSCTF.dll
Opens: C:\WINDOWS\system32\MSCTFIME.IME
Opens: C:\WINDOWS\Fonts\sserife.fon
Opens: C:\WINDOWS\system32\MSIMTF.dll
Writes to: C:\Documents and Settings\Admin\Local Settings\Temp\cpuz_x32.sys
Deletes: C:\Documents and Settings\Admin\Local Settings\Temp\cpuz_x32.sys

Windows Registry Events

Creates key: HKCU\software\perfmonitor applications
Creates key: HKCU\software\perfmonitor applications\perfmonitor
Creates key: HKCU\software\perfmonitor applications\perfmonitor\recent file list
Creates key: HKCU\software\perfmonitor applications\perfmonitor\settings
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\906eb2c5b0eee128a609c1bae001562f.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\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\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\winspool.drv
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\winmm.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: 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\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 nt\currentversion\drivers32
Opens key: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm
Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
Opens key: HKCU\software\microsoft\windows\currentversion\policies\network
Opens key: HKCU\software\microsoft\windows\currentversion\policies\comdlg32
Opens key: HKLM\system\currentcontrolset\control\computername
Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
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\906eb2c5b0eee128a609c1bae001562f.exe\rpcthreadpoolthrottle
Opens key: HKLM\software\policies\microsoft\windows nt\rpc
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\powrprof.dll
Opens key: HKCU\control panel\powercfg
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg

Opens key: HKCU\control panel\powercfg\powerpolicies
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies
Opens key: HKCU\control panel\powercfg\powerpolicies\0
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\0
Opens key: HKCU\control panel\powercfg\powerpolicies\1
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\1
Opens key: HKCU\control panel\powercfg\powerpolicies\2
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\2
Opens key: HKCU\control panel\powercfg\powerpolicies\3
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\3
Opens key: HKCU\control panel\powercfg\powerpolicies\4
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\4
Opens key: HKCU\control panel\powercfg\powerpolicies\5
Opens key: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\5
Opens key: HKCU\software
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msctf.dll
Opens key: HKLM\software\microsoft\ctf\compatibility\906eb2c5b0eee128a609c1bae001562f.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: 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[906eb2c5b0eee128a609c1bae001562f]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime compatibility[906eb2c5b0eee128a609c1bae001562f]
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: 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\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\windows nt\currentversion\drivers32[wave]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[wave9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[midi9]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[aux9]
Queries value: HKLM\system\currentcontrolset\control\mediaproperties\privateproperties\joystick\winmm[wheel]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer4]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer5]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer6]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer7]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer8]
Queries value: HKLM\software\microsoft\windows nt\currentversion\drivers32[mixer9]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nodrives]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[restrictrun]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[nonetconnectdisconnect]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[norecentdocshistory]
Queries value: HKCU\software\microsoft\windows\currentversion\policies\explorer[noclose]
Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
Queries value: HKCU\control panel\powercfg[adminmaxsleep]
Queries value: HKCU\control panel\powercfg[adminmaxvideotimeout]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg[lastid]
Queries value: HKCU\control panel\powercfg\powerpolicies\0[name]

Queries value: HKCU\control panel\powercfg\powerpolicies\0[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\0[policies]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\0[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\1[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\1[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\1[policies]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\1[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\2[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\2[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\2[policies]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\2[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\3[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\3[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\3[policies]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\3[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\4[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\4[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\4[policies]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\4[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\5[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\5[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\5[policies]
Queries value: HKLM\software\microsoft\windows\currentversion\controls folder\powercfg\powerpolicies\5[policies]
Queries value: HKCU\software\perfmonitor applications\perfmonitor\recent file list[file1]
Queries value: HKCU\software\perfmonitor applications\perfmonitor\recent file list[file2]
Queries value: HKCU\software\perfmonitor applications\perfmonitor\recent file list[file3]
Queries value: HKCU\software\perfmonitor applications\perfmonitor\recent file list[file4]
Queries value: HKCU\software\perfmonitor applications\perfmonitor\settings[previewpages]
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]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]