

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 89, Task ID: 357

Task ID:	357
Risk Level:	8
Date Processed:	2016-04-28 12:56:58 (UTC)
Processing Time:	63.22 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:\Users\Admin\AppData\Local\Temp\cpuz_x64.sys]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\BaseNamedObjects\CPUIDSDK
Creates mutex:	\BaseNamedObjects\cpuz
Creates mutex:	\Sessions\1\BaseNamedObjects\PERFMON0
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\BaseNamedObjects\SvcctrlStartEvent_A3752DX
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\cpuz_x64.sys
Opens:	C:\Windows\Prefetch\906EB2C5B0EEE128A609C1BAE0015-D9C78F78.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll

Opens: C:\Windows\system32\wow64log.dll
 Opens: C:\Windows\SysWOW64
 Opens: C:\Windows\SysWOW64\sechost.dll
 Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.Local\
 Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
 controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
 Opens: C:\Windows\winsxs\x86_microsoft.windows.common-
 controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
 Opens: C:\windows\temp\WINSPOOL.DRV
 Opens: C:\Windows\SysWOW64\winspool.drv
 Opens: C:\windows\temp\WINMM.dll
 Opens: C:\Windows\SysWOW64\winmm.dll
 Opens: C:\windows\temp\VERSION.dll
 Opens: C:\Windows\SysWOW64\version.dll
 Opens: C:\Windows\SysWOW64\imm32.dll
 Opens: C:\Windows\SysWOW64\uxtheme.dll
 Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.2.Manifest
 Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.3.Manifest
 Opens: C:\windows\temp\906eb2c5b0eee128a609c1bae001562f.exe.Config
 Opens: C:\Windows\Temp\906eb2c5b0eee128a609c1bae001562f.exe
 Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
 Opens: C:\Users\Admin\AppData\Local\Temp\cpuz_x64.sys
 Opens: C:\windows\temp\PowrProf.dll
 Opens: C:\Windows\SysWOW64\powrprof.dll
 Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui
 Opens: C:\Windows\SysWOW64\PerfMonitor0.ini
 Opens: C:\windows\temp\dwmapapi.dll
 Opens: C:\Windows\SysWOW64\dwmapapi.dll
 Opens: C:\Windows\Fonts\StaticCache.dat
 Opens: C:\Windows\Fonts\sserife.fon
 Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui
 Opens: C:\Windows\SysWOW64\ole32.dll
 Opens: C:\Windows\SysWOW64\rpcss.dll
 Opens: C:\Windows\Fonts\arial.ttf
 Writes to: C:\Users\Admin\AppData\Local\Temp\cpuz_x64.sys
 Reads from: C:\Windows\Fonts\StaticCache.dat
 Deletes: C:\Users\Admin\AppData\Local\Temp\cpuz_x64.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
 Opens key: HKLM\system\currentcontrolset\control\session manager
 Opens key: HKLM\software\microsoft\wow64
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
 execution options
 Opens key: HKLM\system\currentcontrolset\control\terminal server
 Opens key: HKLM\system\currentcontrolset\control\safeboot\option
 Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
 Opens key:
 HKLM\software\wow6432node\policies\microsoft\windows\safer\codeidentifiers
 Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
 Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
 Opens key: HKLM\system\currentcontrolset\control\nls\language
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us
 Opens key: HKLM\system\currentcontrolset\control\mui\uilanguages\pendingdelete
 Opens key: HKLM\software\wow6432node\policies\microsoft\mui\settings
 Opens key: HKLM\software\policies\microsoft\mui\settings

Opens key: HKCU\
 Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
 Opens key: HKLM\system\currentcontrolset\control\mui\settings\languageconfiguration
 Opens key: HKCU\software\policies\microsoft\control panel\desktop
 Opens key: HKCU\control panel\desktop\languageconfiguration
 Opens key: HKCU\control panel\desktop
 Opens key: HKCU\control panel\desktop\muicached
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside
 Opens key:
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key: HKLM\
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\diagnostics
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\gre_initialize
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\compatibility32
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\ime
 compatibility
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
 Opens key: HKLM\software\wow6432node\microsoft\ole
 Opens key: HKLM\software\wow6432node\microsoft\ole\tracing
 Opens key: HKLM\software\microsoft\ole\tracing
 Opens key: HKLM\software\wow6432node\microsoft\oleaut
 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\system\setup
 Opens key: HKLM\software\wow6432node\microsoft\rpc
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\sqmclient\windows
 Opens key: HKLM\software\microsoft\sqmclient\windows
 Opens key: HKLM\system\currentcontrolset\control\sqmservicelist
 Opens key: HKLM\system\currentcontrolset\control\cmf\config
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\setup
 Opens key: HKLM\software\microsoft\windows\currentversion\setup
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
 Opens key: HKCU\control panel\powercfg\powerpolicies
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
 folder\powercfg\powerpolicies
 Opens key: HKCU\control panel\powercfg\powerpolicies\0
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
 folder\powercfg\powerpolicies\0
 Opens key: HKCU\control panel\powercfg\powerpolicies\1
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
 folder\powercfg\powerpolicies\1
 Opens key: HKCU\control panel\powercfg\powerpolicies\2
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
 folder\powercfg\powerpolicies\2
 Opens key: HKCU\control panel\powercfg\powerpolicies\3
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
 folder\powercfg\powerpolicies\3
 Opens key: HKCU\control panel\powercfg\powerpolicies\4
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
 folder\powercfg\powerpolicies\4
 Opens key: HKCU\control panel\powercfg\powerpolicies\5
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\controls

folder\powercfg\powerpolicies\5
 Opens key: HKCU\software
 Opens key: HKLM\system\currentcontrolset\control\nls\locale
 Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
 Opens key: HKLM\system\currentcontrolset\control\nls\language groups
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\datastore_v1.0
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback\segoe ui
 Opens key:
 HKLM\software\wow6432node\microsoft\ctf\compatibility\906eb2c5b0eee128a609c1bae001562f.exe
 Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options[disableusermodecallbackfilter]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[cwdillegalindllsearch]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[empty]
 Queries value:
 HKLM\system\currentcontrolset\control\nls\language[installlanguagefallback]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-us[type]
 Queries value: HKLM\system\currentcontrolset\control\mui\uilanguages\en-
 us[alternatecodepage]
 Queries value: HKCU\control panel\desktop[preferreduilanguages]
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
 Queries value:
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\compatibility32[906eb2c5b0eee128a609c1bae001562f]
 Queries value: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\windows[loadappinit_dlls]
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
 Queries value:
 HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value: HKLM\system\setup[oobeinprogress]
 Queries value: HKLM\system\setup\systemsetupinprogress]
 Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value: HKLM\system\currentcontrolset\control\sqmservicelist[sqmservicelist]
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
 reporting\wmr[disable]
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
 Queries value: HKCU\control panel\powercfg\powerpolicies\0[description]

Queries value: HKCU\control panel\powercfg\powerpolicies\0[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\0[policies]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
folder\powercfg\powerpolicies\0[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\1[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\1[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\1[policies]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
folder\powercfg\powerpolicies\1[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\2[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\2[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\2[policies]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
folder\powercfg\powerpolicies\2[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\3[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\3[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\3[policies]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
folder\powercfg\powerpolicies\3[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\4[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\4[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\4[policies]
Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion\controls
folder\powercfg\powerpolicies\4[policies]
Queries value: HKCU\control panel\powercfg\powerpolicies\5[description]
Queries value: HKCU\control panel\powercfg\powerpolicies\5[name]
Queries value: HKCU\control panel\powercfg\powerpolicies\5[policies]
Queries value: HKLM\software\wow6432node\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\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]

Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]