

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 62, Task ID: 248

Task ID:	248
Risk Level:	1
Date Processed:	2016-04-28 12:53:57 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.exe"
Sample ID:	62
Type:	basic
Owner:	admin
Label:	96b8137418767d16c5b80d9f28cff9c4
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	768000 bytes
MD5:	96b8137418767d16c5b80d9f28cff9c4
SHA256:	15b751c98d1f3197a60bdc32483e9038ec6ab301d0710d84bb732e35084b54a6
Description:	None

## Pattern Matching Results

### Static Events

Anomaly:	PE: Contains a virtual section
----------	--------------------------------

### Process/Thread Events

Creates process:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.exe
["C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.exe" ]	

### Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfdMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfdActivated.Default1

### File System Events

Creates:	C:\Windows\Temp\96b8137418767d16c5b80d9f28cff9c4.ext
Opens:	C:\Windows\Prefetch\96B8137418767D16C5B80D9F28CFF-B3FF606A.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\msimg32.dll
Opens:	C:\Windows\System32\msimg32.dll
Opens:	C:\windows\temp\version.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll	
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.ENU
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.ENU.DLL
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.EN
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.EN.DLL
Opens:	C:\Windows\System32\uxtheme.dll

Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.exe
Opens:	C:\Windows\Temp
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.exe.log
Opens:	C:\windows\temp\96b8137418767d16c5b80d9f28cff9c4.batch-chm2doc
Opens:	C:\Windows\System32\en-US\KernelBase.dll.mui
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\system32\uxtheme.dll.Config
Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\winsxs\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui	
Opens:	C:\Windows\Fonts\verdana.ttf
Opens:	C:\Windows\Fonts\verdanab.ttf
Writes to:	C:\Windows\Temp\96b8137418767d16c5b80d9f28cff9c4.exe
Reads from:	C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\ddl
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
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\microsoft\windows\currentversion\sidebyside
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
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\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKLM\software\microsoft\ole\tracing
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKCU\software\borland\locales
Opens key:	HKLM\software\borland\locales
Opens key:	HKCU\software\borland\delphi\locales
Opens key:	HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key:	HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
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\system\currentcontrolset\control\cmf\config  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\tahoma  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\verdana  
 Opens key:  
 HKLM\software\microsoft\ctf\compatibility\96b8137418767d16c5b80d9f28cff9c4.exe  
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
 Opens key: HKLM\software\microsoft\ctf\  
 Opens key: HKLM\software\microsoft\ctf\knownclasses  
 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: HKCU\control panel\desktop[preferreduilanguages]  
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
 Queries value:  
 HKLM\software\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\microsoft\windows  
 nt\currentversion\compatibility32[96b8137418767d16c5b80d9f28cff9c4]  
 Queries value: HKLM\software\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\nls\customlocale[en-us]  
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
 Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms  
 shell dlg 2]  
 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\system\currentcontrolset\control\cmf\config[system]  
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-  
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]  
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]