

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 187, Task ID: 746

Task ID:	746
Risk Level:	1
Date Processed:	2016-04-28 13:08:06 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\256ca69b89f0afc1f54c82efa1ae33d.exe"
Sample ID:	187
Type:	basic
Owner:	admin
Label:	256ca69b89f0afc1f54c82efa1ae33d
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	745984 bytes
MD5:	256ca69b89f0afc1f54c82efa1ae33d
SHA256:	dee91f4b85f5750d72ff874b8d0226b18e9157436b9a5bc142d0296e039df87c
Description:	None

## Pattern Matching Results

### Static Events

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

### Process/Thread Events

Creates process:	C:\windows\temp\256ca69b89f0afc1f54c82efa1ae33d.exe
["C:\windows\temp\256ca69b89f0afc1f54c82efa1ae33d.exe" ]	

### Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	---

### File System Events

Opens:	C:\Windows\Prefetch\256CA69B89F0AFCF1F54C82EFA1AE-C9229DDB.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\256ca69b89f0afc1f54c82efa1ae33d.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll	
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll
Opens:	C:\Windows\SysWOW64\rpcrt4.dll

Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\dwmmapi.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_5.82.9200.16384_en-us_d51b55b9729b0b41	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.c..-
controls.resources_6595b64144ccf1df_5.82.9200.16384_en-us_d51b55b9729b0b41\comctl32.dll.mui	
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\SysWOW64\uxtheme.dll.Config
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll	
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\Temp
Reads from:	C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

Creates key:	HKCU\software\emptyfileremover
Opens key:	HKLM\software\microsoft\wow64
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\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags\dbglog
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\disable8and16bitmitigation	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	
HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnsoptions	

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\  
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows  
Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy  
Opens key: HKLM\system\currentcontrolset\control\lsa  
Opens key: HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration  
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\borland\locales  
Opens key: HKLM\software\wow6432node\borland\locales  
Opens key: HKCU\software\borland\delphi\locales  
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
Opens key: HKLM\software\policies\microsoft\sqmclient\windows  
Opens key: HKLM\software\microsoft\sqmclient\windows  
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation  
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids  
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\languagepack\datastore\_v1.0  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback\ms sans serif  
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink  
Opens key: HKLM\software\microsoft\windows  
nt\currentversion\languagepack\surrogatefallback\segoe ui  
Opens key: HKCU\software\emptyfileremover  
Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\256ca69b89f0afc1f54c82efa1ae33d.exe  
Opens key: HKLM\software\wow6432node\microsoft\ctf\  
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses  
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: HKCU\software\microsoft\windows  
nt\currentversion\appcompatflags[showdebuginfo]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
options\dllnsoptions[usefilter]  
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\dlloptions[256ca69b89f0afc1f54c82efa1ae33d.exe]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[256ca69b89f0afc1f54c82efa1ae33d]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]  
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
Queries value: HKLM\software\microsoft\ole[aggressivemtesting]  
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
reporting\wmr[disable]  
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]  
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: HKCU\software\emptyfileremover[tt]  
Queries value: HKCU\software\emptyfileremover[bb]  
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]  
Sets/Creates value: HKCU\software\emptyfileremover[bb]