

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 3307, Task ID: 738

Task ID:	738
Risk Level:	6
Date Processed:	2016-05-18 10:32:30 (UTC)
Processing Time:	14.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6b78f38317a53920e530cc1e36053242.exe"
Sample ID:	3307
Type:	basic
Owner:	admin
Label:	6b78f38317a53920e530cc1e36053242
Date Added:	2016-05-18 10:30:48 (UTC)
File Type:	PE32:win32:gui
File Size:	407933 bytes
MD5:	6b78f38317a53920e530cc1e36053242
SHA256:	cd43eae17643cd5510d87ca5b49ddb5b45f73b83c169dcd1102b356633943046
Description:	None

## Pattern Matching Results

5	PE: Contains compressed section
6	Packer: PECompact
2	PE: Nonstandard section

## Static Events

Anomaly:	PE: Contains one or more non-standard sections
Packer:	PeCompact

## Process/Thread Events

Creates process:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe
["C:\windows\temp\6b78f38317a53920e530cc1e36053242.exe" ]	

## Named Object Events

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

## File System Events

Opens:	C:\Windows\Prefetch\6B78F38317A53920E530CC1E36053-7800A4C9.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\version.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.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\winmm.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.ENU

Opens:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.ENU.DLL
Opens:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.EN
Opens:	C:\windows\temp\6b78f38317a53920e530cc1e36053242.EN.DLL
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\dwmapl.dll
Opens:	C:\Windows\SysWOW64\dwmapl.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

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\ddl
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\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\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  
 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[6b78f38317a53920e530cc1e36053242]  
 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\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\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]