

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 96, Task ID: 385

Task ID:	385
Risk Level:	1
Date Processed:	2016-04-28 12:57:36 (UTC)
Processing Time:	61.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e5cd011aa053b4d825844332db22f1b2.exe"
Sample ID:	96
Type:	basic
Owner:	admin
Label:	e5cd011aa053b4d825844332db22f1b2
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	840344 bytes
MD5:	e5cd011aa053b4d825844332db22f1b2
SHA256:	c2b2644c913407ba97a06fc852d7319359bf0b3c0e6155fac53c91b33c13f634
Description:	None

## Pattern Matching Results

### Static Events

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

### Process/Thread Events

Creates process:	C:\windows\temp\e5cd011aa053b4d825844332db22f1b2.exe
	["C:\windows\temp\e5cd011aa053b4d825844332db22f1b2.exe" ]

### File System Events

Opens:	C:\Windows\Prefetch\E5CD011AA053B4D825844332DB22F-5131D27B.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\e5cd011aa053b4d825844332db22f1b2.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\winpool.drv
Opens:	C:\Windows\SysWOW64\winpool.drv
Opens:	C:\windows\temp\GrafikRW.DLL
Opens:	C:\Windows\SysWOW64\GrafikRW.DLL
Opens:	C:\Windows\system\GrafikRW.DLL
Opens:	C:\Windows\GrafikRW.DLL
Opens:	C:\Windows\SysWOW64\Wbem\GrafikRW.DLL
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\GrafikRW.DLL

### 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\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  
 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]