

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 206, Task ID: 825

Task ID:	825
Risk Level:	1
Date Processed:	2016-04-28 13:10:00 (UTC)
Processing Time:	62.12 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7f5a985a8a280d8fff703341af3baa0a.exe"
Sample ID:	206
Type:	basic
Owner:	admin
Label:	7f5a985a8a280d8fff703341af3baa0a
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	299008 bytes
MD5:	7f5a985a8a280d8fff703341af3baa0a
SHA256:	7054d2ace3b9b6930fc01046cb09f843145dcc12b3ec8630652e49be6e2faf fb
Description:	None

## Pattern Matching Results

## Process/Thread Events

Creates process:	C:\windows\temp\7f5a985a8a280d8fff703341af3baa0a.exe
["C:\windows\temp\7f5a985a8a280d8fff703341af3baa0a.exe" ]	

## File System Events

Opens:	C:\Windows\Prefetch\7F5A985A8A280D8FFF703341AF3BA-8C135ED0.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\temp\WINMM.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\Popups.dll
Opens:	C:\Windows\SysWOW64\Popups.dll
Opens:	C:\Windows\system\Popups.dll
Opens:	C:\Windows\Popups.dll
Opens:	C:\Windows\SysWOW64\Wbem\Popups.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Popups.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  
 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]