

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 244, Task ID: 974

Task ID:	974
Risk Level:	6
Date Processed:	2016-04-28 13:14:18 (UTC)
Processing Time:	61.53 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\d0cf7e0774812903c07c433428f9418d.exe"
Sample ID:	244
Type:	basic
Owner:	admin
Label:	d0cf7e0774812903c07c433428f9418d
Date Added:	2016-04-28 12:45:15 (UTC)
File Type:	PE32:win32:gui
File Size:	264704 bytes
MD5:	d0cf7e0774812903c07c433428f9418d
SHA256:	cc3c1000a1b1226a49576a1eff5edd601de762001be5a0b4c2796340b5213469
Description:	None

## Pattern Matching Results

- 6 PE: File has TLS callbacks
- 2 PE: Nonstandard section

## Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Anomaly:	PE: File contain TLS callbacks

## Process/Thread Events

Creates process:	C:\windows\temp\d0cf7e0774812903c07c433428f9418d.exe
["C:\windows\temp\d0cf7e0774812903c07c433428f9418d.exe" ]	

## Named Object Events

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

## File System Events

Opens:	C:\Windows\Prefetch\D0CF7E0774812903C07C433428F94-FBB65E1F.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\d0cf7e0774812903c07c433428f9418d.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

## Windows Registry Events

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  
 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]