

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 152, Task ID: 606

Task ID:	606
Risk Level:	1
Date Processed:	2016-04-28 13:03:34 (UTC)
Processing Time:	61.17 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\e8fcc1e157e865519dd42edea53b1a53.exe"
Sample ID:	152
Type:	basic
Owner:	admin
Label:	e8fcc1e157e865519dd42edea53b1a53
Date Added:	2016-04-28 12:45:06 (UTC)
File Type:	PE32:win32:gui
File Size:	52544 bytes
MD5:	e8fcc1e157e865519dd42edea53b1a53
SHA256:	1f094c241fbefd8ac33e0ef5508cf51a94d05cbc5154a94a74fef0435de09c02
Description:	None

## Pattern Matching Results

### Static Events

Anomaly: PE: Contains a virtual section

### Process/Thread Events

Creates process: C:\windows\temp\e8fcc1e157e865519dd42edea53b1a53.exe  
["C:\windows\temp\e8fcc1e157e865519dd42edea53b1a53.exe" ]

### Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

### File System Events

Opens: C:\Windows\Prefetch\E8FCC1E157E865519DD42EDEA53B1-3BDC4F98.pf  
Opens: C:\Windows  
Opens: C:\Windows\System32\wow64.dll  
Opens: C:\Windows\SysWOW64  
Opens: C:\Windows\SysWOW64\apphelp.dll  
Opens: C:\Windows\Temp\e8fcc1e157e865519dd42edea53b1a53.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\ntp\customlocale  
Opens key: HKLM\system\currentcontrolset\control\ntp\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]