

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 231, Task ID: 922

Task ID:	922
Risk Level:	5
Date Processed:	2016-04-28 13:12:40 (UTC)
Processing Time:	2.35 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\0b0c9ef614d272f727f360736fa53c7c.exe"
Sample ID:	231
Type:	basic
Owner:	admin
Label:	0b0c9ef614d272f727f360736fa53c7c
Date Added:	2016-04-28 12:45:14 (UTC)
File Type:	PE32:win32:gui
File Size:	67472 bytes
MD5:	0b0c9ef614d272f727f360736fa53c7c
SHA256:	aaf6ea32a1afd1c85e3081c717820b4dd326be53d3f38034c0f87aa514af98b1
Description:	None

## Pattern Matching Results

- 2 PE: Nonstandard section
- 5 Packer: UPX
- 4 Checks whether debugger is present
- 5 PE: Contains compressed section

## Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	UPX

## Process/Thread Events

Creates process:	C:\windows\temp\0b0c9ef614d272f727f360736fa53c7c.exe
["C:\windows\temp\0b0c9ef614d272f727f360736fa53c7c.exe" ]	
Terminates process:	C:\Windows\Temp\0b0c9ef614d272f727f360736fa53c7c.exe

## Named Object Events

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

## File System Events

Opens:	C:\Windows\Prefetch\0B0C9EF614D272F727F360736FA53-25FB CD08.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\0b0c9ef614d272f727f360736fa53c7c.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\appatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\b cryptprimitives.dll
Opens:	C:\Windows\SysWOW64\cryptbase.dll
Opens:	C:\Windows\SysWOW64\sspicli.dll

Opens:	C:\Windows\SysWOW64\rpcrt4.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\cfgmgr32.dll
Opens:	C:\Windows\SysWOW64\devobj.dll
Opens:	C:\Windows\SysWOW64\setupapi.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll

## 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\srb\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\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\lsa\fipsalgorithmpolicy
Opens key:	HKLM\system\currentcontrolset\control\lsa
Opens key:	HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
Opens key:	HKLM\
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\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\windows\windows error reporting\wmr
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion\setup
Opens key:	HKLM\software\microsoft\windows\currentversion\setup
Opens key:	HKLM\software\wow6432node\microsoft\windows\currentversion
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

Queries value: HKLM\system\currentcontrolset\control\terminal server[tserverenabled]  
 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\lsa\fipsalgorithmpolicy[enabled]  
 Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]  
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
 Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]  
 Queries value: HKLM\software\microsoft\windows\nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\wow6432node\microsoft\windows\nt\currentversion\compatibility32[0b0c9ef614d272f727f360736fa53c7c]  
 Queries value: HKLM\software\wow6432node\microsoft\windows\nt\currentversion\windows[loadappinit\_dlls]  
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]  
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]  
 Queries value: HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]  
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]