

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 205, Task ID: 818	
Task ID:	818
Risk Level:	4
Date Processed:	2016-04-28 13:09:58 (UTC)
Processing Time:	15.52 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.exe"
Sample ID:	205
Type:	basic
Owner:	admin
Label:	7fb29afcdb4ab59eea2314061136ed82
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	146944 bytes
MD5:	7fb29afcdb4ab59eea2314061136ed82
SHA256:	f53388af47c8e24680dedebc4c5d2eb6434fdf5d4bb3c1efb0a41c8e4a22b771
Description:	None

## Pattern Matching Results

- 4 Reads process memory
- 2 Terminates third-party processes

## Static Events

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

## Process/Thread Events

Creates process:	C:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.exe
["C:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.exe" ]	
Creates process:	C:\Program Files\Java\jre7\launch4j-tmp\7fb29afcdb4ab59eea2314061136ed82.exe ["C:\Program Files\Java\jre7\launch4j-tmp\7fb29afcdb4ab59eea2314061136ed82.exe" -Xmx512M -Xss5M -classpath "lib\RationalPlan.jar;lib\RationalPlan.jar;lib\swingx.jar;lib\datepicker.jar;lib\datepicker-i18n.jar;lib\jlfgr-1.0.jar;lib\looks.jar;lib\itext.jar;lib\jxl.jar;lib\AppleJavaExtensions.jar;lib\mpxj.jar;lib\mail.jar;lib\activation.jar;lib\ical4j.jar;lib\commons-logging.jar;lib\commons-lang.jar;lib\poi.jar;lib\quaqu.jar;lib\jaxb-api.jar;lib\jaxb-impl.jar;lib\jsr173_1.0_api.jar;lib\spring.jar;lib\spring-webmvc.jar;lib\swing-worker-1.2.jar;lib\jasperreports.jar;lib\jasperreports-fonts-4.0.1.jar;lib\groovy-all.jar;lib\commons-collections-3.2.1.jar;lib\commons-digester-2.1.jar;lib\SHEF.jar;lib\sam.jar;lib\jtidy.jar;lib\novaworx-syntax.jar;lib\jna.jar;lib\jayatana.jar;lib\dropbox-java-sdk.jar;lib\httpmime.jar;lib\httpclient.jar;lib\httpcore.jar;lib\json_simple.jar;lib\google-api-client.jar;lib\google-api-services-drive.jar;lib\google-http-client.jar;lib\google-oauth-client.jar;lib\guava.jar;lib\jackson-core-asl.jar;lib\resources" com.sbs.jpmain]
Reads from process:	PID:2876 C:\Program Files\Java\jre7\launch4j-tmp\7fb29afcdb4ab59eea2314061136ed82.exe
Writes to process:	PID:2876 C:\Program Files\Java\jre7\launch4j-tmp\7fb29afcdb4ab59eea2314061136ed82.exe
Terminates process:	C:\Program Files\Java\jre7\launch4j-tmp\7fb29afcdb4ab59eea2314061136ed82.exe
Terminates process:	C:\Windows\Temp\7fb29afcdb4ab59eea2314061136ed82.exe

## Named Object Events

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

## File System Events

Creates:	C:\Program Files\Java\jre7\launch4j-tmp
Creates:	C:\Program Files\Java\jre7\launch4j-tmp\7fb29afcdb4ab59eea2314061136ed82.exe
Creates:	C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
Creates:	C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin\2876
Opens:	C:\Windows\Prefetch\7FB29AFCD4AB59EEA2314061136E-0B9672A4.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\7fb29afcdb4ab59eea2314061136ed82.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
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\bcryptprimitives.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\Temp
Opens:	C:\Program Files\Java\jre7\bin

```

Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens: C:\Program Files\Java\jre7
Opens: C:\Program Files\Java\jre7\bin\javaw.exe
Opens: C:\Program Files\Java\jre7\launch4j-
tmp\7fb29afcdb4ab59eea2314061136ed82.exe
Opens: C:\Windows\SysWOW64\ntmarta.dll
Opens: C:\windows\temp\7fb29afcdb4ab59eea2314061136ed82.l4j.ini
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\apppatch\apppatch64\sysmain.sdb
Opens: C:\Program Files\Java\jre7\launch4j-tmp
Opens: C:\Program Files
Opens: C:\Program Files\Java
Opens: C:\Windows\Prefetch\7FB29AFCD84AB59EEA2314061136E-029327EB.pf
Opens: C:\Windows\System32\apphelp.dll
Opens: C:\Windows\System32\ntdll.dll
Opens: C:\Windows\System32\kernel32.dll
Opens: C:\Windows\System32\KernelBase.dll
Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f
Opens: C:\Windows\WinSxS\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_418c2a697189c07f\comctl32.dll
Opens: C:\Windows\System32\sechost.dll
Opens: C:\Windows\System32\msvcrt.dll
Opens: C:\Windows\System32\rpcrt4.dll
Opens: C:\Windows\System32\advapi32.dll
Opens: C:\Windows\System32\gdi32.dll
Opens: C:\Windows\System32\user32.dll
Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\System32\msctf.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\System32\tzres.dll
Opens: C:\Windows\System32\en-US\tzres.dll.mui
Opens: C:\Program Files\Java\jre7\lib\amd64\jvm.cfg
Opens: C:\Program Files\Java\jre7\bin\server
Opens: C:\Program Files\Java\jre7\bin\msvcr100.dll
Opens: C:\Program Files\Java\jre7\bin\server\jvm.dll
Opens: C:\Windows\System32\wsock32.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\Windows\System32\winmmbase.dll
Opens: C:\Windows\System32\ansi.dll
Opens: C:\Windows\System32\ws2_32.dll
Opens: C:\Windows\System32\psapi.dll
Opens: C:\Program Files\Java\jre7\bin\verify.dll
Opens: C:\Program Files\Java\jre7\bin\java.dll
Opens: C:\hotspotrc
Opens: C:\
Opens: C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
Opens: C:\Program Files\Java\jre7\bin\zip.dll
Opens: C:\Program Files\Java\jre7\lib
Opens: C:\Program Files\Java\jre7\lib\meta-index
Opens: C:\Program Files\Java\jre7\lib\rt.jar
Opens: C:\hotspot_compiler
Opens: C:\Program Files\Java\jre7\lib\ext\meta-index
Opens: C:\Program Files\Java\jre7\lib\ext
Writes to: C:\Program Files\Java\jre7\launch4j-
tmp\7fb29afcdb4ab59eea2314061136ed82.exe
Reads from: C:\Program Files\Java\jre7\bin\javaw.exe
Reads from: C:\Program Files\Java\jre7\lib\amd64\jvm.cfg
Reads from: C:\Program Files\Java\jre7\lib\meta-index
Reads from: C:\Program Files\Java\jre7\lib\rt.jar
Reads from: C:\Program Files\Java\jre7\lib\ext\meta-index

```

## 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\locale
Opens key: HKLM\system\currentcontrolset\control\locale\language
Opens key: HKLM\system\currentcontrolset\control\mui\languages
Opens key: HKLM\system\currentcontrolset\control\mui\languages\en-us
Opens key: HKLM\system\currentcontrolset\control\mui\languages\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\machineconfiguration
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\locale\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\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options

```

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dllexportoptions  
 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\javasoft\java runtime environment  
 Opens key: HKLM\software\javasoft\java development kit  
 Opens key: HKLM\software\wow6432node\javasoft\java development kit  
 Opens key: HKLM\software\javasoft\java runtime environment\1.7.0\_02  
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\system  
 Opens key: HKLM\software\policies\microsoft\windows\system  
 Opens key: HKLM\system\currentcontrolset\control\lsa\accessproviders  
 Opens key: HKLM\software\policies\microsoft\sqlclient\windows  
 Opens key: HKLM\software\microsoft\sqlclient\windows  
 Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\7fb29afcdb4ab59eea2314061136ed82.exe  
 Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls  
 Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility  
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\appcompat  
 Opens key: HKLM\software\policies\microsoft\windows\appcompat  
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers  
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\appcompatflags\custom\7fb29afcdb4ab59eea2314061136ed82.exe  
 Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside  
 Opens key:  
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key: HKLM\system\currentcontrolset\control\error message instrument\  
 Opens key: HKLM\system\currentcontrolset\control\error message instrument  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\windows  
 Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr  
 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[alternatencodepage]  
 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\software\microsoft\windows nt\currentversion\image file execution  
 options\dllexportoptions[usefilter]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dllexportoptions[7fb29afcdb4ab59eea2314061136ed82.exe]  
 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[aggressivemtesting]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\compatibility32[7fb29afcdb4ab59eea2314061136ed82]  
 Queries value: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\windows[loadappinit\_dlls]  
 Queries value: HKLM\software\javasoft\java runtime environment\1.7.0\_02[javahome]  
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
 reporting\wmr[disable]  
 Queries value:  
 HKLM\software\policies\microsoft\windows\system[copyfilebufferedsynchronousio]  
 Queries value:  
 HKLM\system\currentcontrolset\control\lsa\accessproviders[martaextension]  
 Queries value: HKLM\software\policies\microsoft\windows\system[copyfilechunksizes]  
 Queries value: HKLM\software\policies\microsoft\windows\system[copyfileoverlappedcount]  
 Queries value: HKLM\software\microsoft\sqlclient\windows[ceipenable]  
 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]

Queries value:  
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[cache]  
Queries value:  
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\compatibility32[7fb29afcdb4ab59eea2314061136ed82]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\windows[loadappinit\_dlls]  
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell  
folders[desktop]