

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 104, Task ID: 417

Task ID:	417
Risk Level:	4
Date Processed:	2016-04-28 12:58:14 (UTC)
Processing Time:	63.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\00fb2b775408dd440ed23bfdb8c4d61d.exe"
Sample ID:	104
Type:	basic
Owner:	admin
Label:	00fb2b775408dd440ed23bfdb8c4d61d
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	826760 bytes
MD5:	00fb2b775408dd440ed23bfdb8c4d61d
SHA256:	36774a60c4940459eaa2ba290529702f3a1e51fac3303d1935d8ee510cffc94e
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\00fb2b775408dd440ed23bfdb8c4d61d.exe
["C:\windows\temp\00fb2b775408dd440ed23bfdb8c4d61d.exe"]	
Creates process:	c:\PROGRA~2\java\jre7\bin\java.exe [c:\PROGRA~2\java\jre7\bin\java.exe - version]
Terminates process:	C:\PROGRA~2\Java\jre7\bin\java.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates event:	\BaseNamedObjects\ConsoleEvent-0x000000000000006DC
Creates semaphore:	\Sessions\1\BaseNamedObjects\c:_windows_temp_00fb2b775408dd440ed23bfdb8c4d61d.exe

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\
Creates:	C:\Users\Admin\AppData\Local\Temp\e4j4DAD.tmp
Creates:	C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
Creates:	C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin\816
Opens:	C:\Windows\Prefetch\00FB2B775408DD440ED23BFDB8C4D-875A9BAD.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\SysWOW64\sechost.dll
Opens:	C:\windows\temp\00fb2b775408dd440ed23bfdb8c4d61d.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\Temp\00fb2b775408dd440ed23bfdb8c4d61d.exe
Opens: C:\
Opens: C:\Windows\Temp
Opens: C:\Users\Admin\AppData\Local\Temp
Opens: C:\Users
Opens: C:\Users\Admin
Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Local
Opens: C:\Windows\install4j\pref_jre.cfg
Opens: C:\windows\jre\lib\
Opens: C:\windows\jre\jre\bin\
Opens: C:\windows\jre\bin\
Opens: C:\Program Files (x86)\Java\jre7\jre\bin\
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\Fonts\arial.ttf
Opens: C:\Program Files (x86)\Java\jre7\bin
Opens: C:\Program Files (x86)\Java\jre7\bin\java.exe
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\Program Files (x86)
Opens: C:\Program Files (x86)\Java
Opens: C:\Program Files (x86)\Java\jre7
Opens: C:\PROGRA~2\java\jre7\bin\ui\SwDRM.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\jpishare.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\java.dll
Opens: C:\bin\launch.exe
Opens: C:\Windows\Prefetch\JAVA.EXE-69992B3F.pf
Opens: C:\PROGRA~2\java\jre7\bin\java.exe.Local\
Opens: C:\Windows\SysWOW64\tzres.dll
Opens: C:\Windows\SysWOW64\en-US\tzres.dll.mui
Opens: C:\Program Files (x86)\Java\jre7\lib\i386\jvm.cfg
Opens: C:\Program Files (x86)\Java\jre7\bin\client
Opens: C:\Program Files (x86)\Java\jre7\bin\msvcr100.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\client\jvm.dll
Opens: C:\PROGRA~2\java\jre7\bin\WSOCK32.dll
Opens: C:\Windows\SysWOW64\wsck32.dll
Opens: C:\PROGRA~2\java\jre7\bin\WINMM.dll
Opens: C:\Windows\SysWOW64\winmm.dll
Opens: C:\Program Files (x86)\Java\jre7\bin\verify.dll
Opens: C:.hotspotrc
Opens: C:\PROGRA~2\java\jre7\lib\endorsed
Opens: C:\Users\Admin\AppData\Local\Temp\hsperfdata_Admin
Opens: C:\Program Files (x86)\Java\jre7\bin\zip.dll
Opens: C:\Program Files (x86)\Java\jre7\lib
Opens: C:\Program Files (x86)\Java\jre7\lib\meta-index
Opens: C:\Program Files (x86)\Java\jre7\bin\client\classes.jsa
Opens: C:\Program Files (x86)\Java\jre7\lib\rt.jar
Opens: C:.hotspot_compiler
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\meta-index
Opens: C:\Program Files (x86)\Java\jre7\lib\ext
Opens: C:\Windows\Sun\Java\lib\ext\meta-index
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\dnsns.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\localedata.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunec.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunjce_provider.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunmscapi.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\sunpkcs11.jar
Opens: C:\Program Files (x86)\Java\jre7\lib\ext\zipfs.jar

Opens:	C:\Windows\Sun\Java\lib\ext
Opens:	C:\PROGRA~2\java\jre7\lib\management\usagetracker.properties
Opens:	C:\Users\Admin\AppData\Local\Temp\e4j4DAD.tmp
Opens:	C:\program files (x86)\java\jre7\bin\server\
Opens:	C:\program files (x86)\java\jre7\bin\server\jvm.dll
Opens:	C:\program files (x86)\java\jre7\bin\hotspot\
Opens:	C:\program files (x86)\java\jre7\bin\hotspot\jvm.dll
Opens:	C:\windows\temp\WSOCK32.dll
Opens:	C:\windows\temp\WINMM.dll
Opens:	C:\windows\temp\MSVCR100.dll
Opens:	C:\Windows\SysWOW64\msvcr100.dll
Opens:	C:\Windows\Temp\00fb2b775408dd440ed23bfdb8c4d61d.voptions
Opens:	C:\Windows\Temp\00fb2b775408dd440ed23bfdb8c4d61d.exe.voptions
Opens:	C:\Windows\bin\
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\windows\temp\imageres.dll
Opens:	C:\Windows\SysWOW64\imageres.dll
Opens:	C:\Windows\SysWOW64\en-US\imageres.dll.mui
Writes to:	C:\Users\Admin\AppData\Local\Temp\e4j4DAD.tmp
Reads from:	C:\Windows\Temp\00fb2b775408dd440ed23bfdb8c4d61d.exe
Reads from:	C:\Program Files (x86)\Java\jre7\bin\java.exe
Reads from:	C:\Program Files (x86)\Java\jre7\lib\i386\jvm.cfg
Reads from:	C:\Program Files (x86)\Java\jre7\lib\meta-index
Reads from:	C:\Program Files (x86)\Java\jre7\bin\client\classes.jsa
Reads from:	C:\Program Files (x86)\Java\jre7\lib\rt.jar
Reads from:	C:\Program Files (x86)\Java\jre7\lib\ext\meta-index
Reads from:	C:\Users\Admin\AppData\Local\Temp\e4j4DAD.tmp
Reads from:	C:\Windows\Fonts\StaticCache.dat
Deletes:	C:\Users\Admin\AppData\Local\Temp\e4j4DAD.tmp

Windows Registry Events

Creates key:	HKCU\software\ej-technologies\exe4j\pids\
Creates key:	HKCU\software
Creates key:	HKCU\software\ej-technologies
Creates key:	HKCU\software\ej-technologies\exe4j
Creates key:	HKCU\software\ej-technologies\exe4j\pids
Creates key:	HKCU\software\ej-technologies\exe4j\jvms\c:/program files
(x86)/java/jre7/bin/java.exe	
Creates key:	HKCU\software\ej-technologies\exe4j\jvms
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\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
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\customlocale
Opens key:	HKLM\system\currentcontrolset\control\locale\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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
 Opens key: HKLM\
 Opens key: HKLM\software\wow6432node\microsoft\windows
 nt\currentversion\diagnostics
 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\system\currentcontrolset\control\nls\extendedlocale
 Opens key: HKLM\software\wow6432node\javasoft\java development kit
 Opens key: HKLM\software\wow6432node\javasoft\java runtime environment
 Opens key: HKLM\software\wow6432node\javasoft\java runtime environment\1.7
 Opens key:
 HKLM\software\wow6432node\microsoft\ctf\compatibility\00fb2b775408dd440ed23bfdb8c4d61d.exe
 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\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
 0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
 Opens key: HKLM\system\currentcontrolset\control\nls\locale
 Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
 Opens key: HKLM\system\currentcontrolset\control\nls\language groups
 Opens key: HKCU\software\ej-technologies\exe4j\jvms\c:/program files
 (x86)/java/jre7/bin/java.exe
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\java.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\java.exe
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
 Opens key: HKLM\system\currentcontrolset\control\cmf\config
 Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
 Opens key: HKCU\software\ej-technologies\exe4j\locatedjvms\
 Opens key: HKLM\software\wow6432node\ej-technologies\exe4j\locatedjvms\
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\datastore_v1.0
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback
 Opens key: HKLM\software\microsoft\windows
 nt\currentversion\languagepack\surrogatefallback\segoe ui
 Opens key:

```

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
  Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer
  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\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
  Queries value: HKLM\system\currentcontrolset\control\ntp\customlocale[empty]
  Queries value:
HKLM\system\currentcontrolset\control\ntp\language[installlanguagefallback]
  Queries value: HKLM\system\currentcontrolset\control\ntp\uilanguages\en-us[type]
  Queries value: HKLM\system\currentcontrolset\control\ntp\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\ntp\sorting\versions[]
  Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[00fb2b775408dd440ed23bfdb8c4d61d]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value: HKLM\system\currentcontrolset\control\ntp\customlocale[en-us]
  Queries value: HKLM\system\currentcontrolset\control\ntp\extendedlocale[en-us]
  Queries value: HKLM\software\wow6432node\javasoft\java runtime
environment[currentversion]
  Queries value: HKLM\software\wow6432node\javasoft\java runtime
environment\1.7[javahome]
  Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]
  Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
  Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value: HKLM\system\currentcontrolset\control\ntp\locale[00000409]
  Queries value: HKLM\system\currentcontrolset\control\ntp\language groups[1]
  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
nt\currentversion\appcompatflags[{22624cac-fe50-451e-9261-e7f22aab93ec}]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[{22624cac-fe50-451e-9261-e7f22aab93ec}]
  Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options[disablelocaloverride]
  Queries value: HKCU\software\microsoft\windows
nt\currentversion\appcompatflags[showdebuginfo]
  Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[java]
  Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
folders[desktop]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]

```

Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
Sets/Creates value: HKCU\software\ej-
technologies\exe4j\pids[c:\windows\temp\00fb2b775408dd440ed23bfdb8c4d61d.exe]
Sets/Creates value: HKCU\software\ej-technologies\exe4j\jvms\c:/program files
(x86)/java/jre7/bin/java.exe[lastwritetime]
Sets/Creates value: HKCU\software\ej-technologies\exe4j\jvms\c:/program files
(x86)/java/jre7/bin/java.exe[version]