

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 177, Task ID: 706

Task ID:	706
Risk Level:	4
Date Processed:	2016-04-28 13:06:35 (UTC)
Processing Time:	61.52 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\5a9a02cb1354aa5e5a938be65387a681.exe"
Sample ID:	177
Type:	basic
Owner:	admin
Label:	5a9a02cb1354aa5e5a938be65387a681
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	16776 bytes
MD5:	5a9a02cb1354aa5e5a938be65387a681
SHA256:	3cdf709240bee9f95cce33f818e494e3bb120493e5a186977640c91822e00c5
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\windows\temp\5a9a02cb1354aa5e5a938be65387a681.exe
["C:\windows\temp\5a9a02cb1354aa5e5a938be65387a681.exe" ]	

## Named Object Events

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

## File System Events

Opens:	C:\Windows\Prefetch\5A9A02CB1354AA5E5A938BE65387A-3817A492.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\5a9a02cb1354aa5e5a938be65387a681.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\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6871_none_50944e7cbcb706e5	
Opens:	
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6871_none_50944e7cbcb706e5\msvcpr90.dll	
Opens:	
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6871_none_50944e7cbcb706e5\msvcr90.dll	
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.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\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\
Opens:	C:\Windows\SysWOW64\SHCore.dll

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls  
Opens: C:\Windows\Fonts\StaticCache.dat  
Opens: C:\Windows\SysWOW64\uxtheme.dll  
Opens: C:\Windows\SysWOW64\dwmapi.dll  
Opens: C:\Windows\SysWOW64\ole32.dll  
Opens: C:\Windows\SysWOW64\oleaut32.dll  
Reads from: C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

Opens key: HKLM\software\microsoft\wow64  
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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
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\  
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows  
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\software\wow6432node\microsoft\ole  
Opens key: HKLM\software\wow6432node\microsoft\ole\tracing  
Opens key: HKLM\software\microsoft\ole\tracing  
Opens key: HKLM\system\currentcontrolset\control\session manager  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-  
238f-46af-adb4-6c85480369c7}  
Opens key:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-  
238f-46af-adb4-6c85480369c7}\propertybag  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1  
Opens key:  
HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\1\knownfolders  
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell

## folders

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids  
Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\knownfolderssettings  
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr  
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: 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\policies\microsoft\sqmclient\windows  
Opens key: HKLM\software\microsoft\sqmclient\windows  
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation  
Opens key:

HKLM\software\wow6432node\microsoft\ctf\compatibility\5a9a02cb1354aa5e5a938be65387a681.exe  
Opens key: HKLM\software\wow6432node\microsoft\ctf\  
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\software\microsoft\windows

nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32[5a9a02cb1354aa5e5a938be65387a681]  
Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]  
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[pageallocatorusesystemheapprivate]  
Queries value: HKLM\software\microsoft\ole[aggressivememtesting]  
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[category]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[name]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[parentfolder]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[description]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[relativepath]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[parsingsname]  
Queries value:

HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[infotip]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localizedname]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[icon]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[security]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[streamresource]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[streamresourcetype]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[localredirectonly]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[roamable]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[precreate]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[stream]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[publishexpandedpath]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[attributes]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[foldertypeid]  
Queries value:  
HKLM\software\wow6432node\microsoft\windows\currentversion\explorer\folderdescriptions\{fdd39ad0-238f-46af-adb4-6c85480369c7}[initfolderhandler]  
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell  
folders[personal]  
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]  
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\ids[en]  
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
reporting\wmr[disable]  
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]  
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]  
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\sqmclient\windows[ceipenable]  
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]