

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 52, Task ID: 208

Task ID:	208
Risk Level:	4
Date Processed:	2016-04-28 12:53:04 (UTC)
Processing Time:	61.32 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe"
Sample ID:	52
Type:	basic
Owner:	admin
Label:	60cd6e1de7fbabcb8f68309beebb124e
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	507904 bytes
MD5:	60cd6e1de7fbabcb8f68309beebb124e
SHA256:	1ead5cb4c8bbf26f95e278fa05256f07fe11e23bb87a9f94311c0c4a5acf0527
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process: C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe  
["C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe" ]

## Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex  
Creates mutex: \Sessions\1\BaseNamedObjects\MetropolisSoftwareGame  
Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0  
Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfdMonitorInstMutexDefault1  
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfdActivated.Default1

## File System Events

Opens: C:\Windows\Prefetch\60CD6E1DE7FBABCB8F68309BEEBB1-A2028995.pf  
Opens: C:\Windows\System32  
Opens: C:\windows\temp\WINSPOOL.DRV  
Opens: C:\Windows\System32\winpool.drv  
Opens: C:\Windows\System32\sechost.dll  
Opens: C:\Windows\System32\apphelp.dll  
Opens: C:\Windows\AppPatch\sysmain.sdb  
Opens: C:\Windows\Temp\60cd6e1de7fbabcb8f68309beebb124e.exe  
Opens: C:\Windows\AppPatch\AcGenral.dll  
Opens: C:\windows\temp\SspiCli.dll  
Opens: C:\Windows\System32\sspicli.dll  
Opens: C:\windows\temp\UxTheme.dll  
Opens: C:\Windows\System32\uxtheme.dll  
Opens: C:\windows\temp\WINMM.dll  
Opens: C:\Windows\System32\winmm.dll  
Opens: C:\windows\temp\samcli.dll  
Opens: C:\Windows\System32\samcli.dll  
Opens: C:\windows\temp\MSACM32.dll  
Opens: C:\Windows\System32\msacm32.dll  
Opens: C:\windows\temp\VERSION.dll  
Opens: C:\Windows\System32\version.dll  
Opens: C:\windows\temp\sfc.dll

Opens:	C:\Windows\System32\sfc.dll
Opens:	C:\windows\temp\sfc_os.DLL
Opens:	C:\Windows\System32\sfc_os.dll
Opens:	C:\windows\temp\USERENV.dll
Opens:	C:\Windows\System32\userenv.dll
Opens:	C:\windows\temp\profapi.dll
Opens:	C:\Windows\System32\profapi.dll
Opens:	C:\windows\temp\dmwapi.dll
Opens:	C:\Windows\System32\dmwapi.dll
Opens:	C:\windows\temp\MPR.dll
Opens:	C:\Windows\System32\mpr.dll
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.Config
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\en-US\setupapi.dll.mui
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.2.Manifest
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.3.Manifest
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af	
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll	
Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\system32\UxTheme.dll.Config
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\WindowsShell.Manifest
Opens:	C:\lang.txt
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Reads from:	C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\ddl
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\
Opens key:	HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key:	HKLM\software\policies\microsoft\mui\settings
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\microsoft\windows\currentversion\sidebyside
Opens key:	HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key:	HKLM\software\policies\microsoft\windows nt\windows file protection
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\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\windows
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics

Opens key: HKLM\software\microsoft\ole  
 Opens key: HKLM\software\microsoft\ole\tracing  
 Opens key: HKLM\software\microsoft\oleaut  
 Opens key: HKLM\system\currentcontrolset\control\cmf\config  
 Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr  
 Opens key: HKLM\software\microsoft\windows\currentversion\setup  
 Opens key: HKLM\software\microsoft\windows\currentversion  
 Opens key: HKLM\system\currentcontrolset\control\nls\customlocale  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 Opens key: HKLM\system\currentcontrolset\services\crypt32  
 Opens key: HKLM\software\microsoft\windows\currentversion\internet settings  
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings  
 Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\network  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\cmdlg32  
 Opens key:  
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 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\microsoft\ctf\compatibility\60cd6e1de7fbabcb8f68309beebb124e.exe  
 Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}  
 Opens key: HKLM\software\microsoft\ctf\  
 Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]  
 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: HKCU\control panel\desktop[preferreduilanguages]  
 Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]  
 Queries value:  
 HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]  
 Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]  
 Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]  
 Queries value: HKLM\software\policies\microsoft\windows nt\windows file protection[knowndlllist]  
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[60cd6e1de7fbabcb8f68309beebb124e]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit\_dlls]  
 Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
 Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]  
 Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
 Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]  
 Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]  
 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\services\crypt32[debugheapflags]  
Queries value: HKLM\software\microsoft\windows\currentversion\internet  
settings[disableimprovedzonecheck]  
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet  
settings[security\_hkml\_only]  
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\ctf\tip\{0000897b-83df-4b96-be07-  
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]  
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]