

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 52, Task ID: 206

Task ID:	206
Risk Level:	4
Date Processed:	2016-04-28 12:52:32 (UTC)
Processing Time:	61.06 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

File System Events

Opens:	C:\Windows\Prefetch\60CD6E1DE7FBABCB8F68309BEEBB1-A2028995.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\60cd6e1de7fbabcb8f68309beebb124e.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\appatch\AcGenral.dll
Opens:	C:\Windows\appatch\AcLayers.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\winmm.dll
Opens:	C:\Windows\SysWOW64\samcli.dll
Opens:	C:\Windows\SysWOW64\msacm32.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\userenv.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\Windows\SysWOW64\winpool.drv
Opens:	C:\Windows\SysWOW64\mpr.dll
Opens:	C:\Windows\SysWOW64\winmmbase.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\profapi.dll

Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\sfc.dll
Opens:	C:\Windows\SysWOW64\sfc_os.dll
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.Config
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\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\urlmon.dll
Opens:	C:\Windows\SysWOW64\cfgmgr32.dll
Opens:	C:\Windows\SysWOW64\devobj.dll
Opens:	C:\Windows\SysWOW64\setupapi.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.2.Manifest
Opens:	C:\windows\temp\60cd6e1de7fbabcb8f68309beebb124e.exe.3.Manifest
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll	
Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\SysWOW64\UxTheme.dll.Config
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985	
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll	
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\Windows\SysWOW64\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\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\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\system\currentcontrolset\control\session manager
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\windows file protection
 Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection
 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\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\software\policies\microsoft\sqmclient\windows
 Opens key: HKLM\software\microsoft\sqmclient\windows
 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\oleaut
 Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
 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
 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\dlloptions
 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\comdlg32
 Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
 Opens key: HKLM\software\wow6432node\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\wow6432node\microsoft\ctf\compatibility\60cd6e1de7fbabcb8f68309beebb124e.exe
 Opens key: HKLM\software\wow6432node\microsoft\ctf\
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
 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[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\session manager[safedllsearchmode]
Queries value: HKLM\software\policies\microsoft\windows nt\windows file
protection[knowndlllist]
Queries value: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[60cd6e1de7fbabcb8f68309beebb124e]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
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\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]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dlloptions[60cd6e1de7fbabcb8f68309beebb124e.exe]
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\wow6432node\microsoft\ctf[enableanchorcontext]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]