

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 64, Task ID: 256

Task ID:	256
Risk Level:	1
Date Processed:	2016-04-28 12:54:07 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe"
Sample ID:	64
Type:	basic
Owner:	admin
Label:	9605ec58da0d3fdca8679abd4c481cc3
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	670328 bytes
MD5:	9605ec58da0d3fdca8679abd4c481cc3
SHA256:	6b8823f2765c3edb6cb59698c7a251607ba2db93a45594f3ce44d141bcd75a9
Description:	None

## Pattern Matching Results

### Static Events

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

### Process/Thread Events

Creates process:	C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe
["C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.exe" ]	
Creates process:	C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp ["C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp"
/SL5="\$6012A,267059,117248,C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.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

### File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp
Creates:	C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp
Opens:	C:\Windows\Prefetch\9605EC58DA0D3FDCA8679ABD4C481-93076565.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.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\System32\imm32.dll
Opens:	C:\Windows\WindowsShell.Manifest
Opens:	C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.ENU
Opens:	C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.ENU.DLL
Opens:	C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.EN

Opens: C:\windows\temp\9605ec58da0d3fdca8679abd4c481cc3.EN.DLL  
 Opens: C:\Windows\System32\en-US\KernelBase.dll.mui  
 Opens: C:\windows\temp\netmsg.dll  
 Opens: C:\Windows\System32\netmsg.dll  
 Opens: C:\Windows\System32\en-US\netmsg.dll.mui  
 Opens: C:\Windows\Temp\9605ec58da0d3fdca8679abd4c481cc3.exe  
 Opens: C:\Users\Admin\AppData\Local\Temp  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp  
 Opens: C:\Windows\Globalization\Sorting\SortDefault.nls  
 Opens: C:\Windows\System32\uxtheme.dll  
 Opens: C:\windows\temp\dwmapi.dll  
 Opens: C:\Windows\System32\dwmapi.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp  
 Opens: C:\Windows\System32\apphelp.dll  
 Opens: C:\Windows\AppPatch\sysmain.sdb  
 Opens: C:\  
 Opens: C:\Users  
 Opens: C:\Users\Admin  
 Opens: C:\Users\Admin\AppData  
 Opens: C:\Users\Admin\AppData\Local  
 Opens: C:\Windows\Prefetch\9605EC58DA0D3FDCA8679ABD4C481-EF577D54.pf  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\msimg32.dll  
 Opens: C:\Windows\System32\msimg32.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\version.dll  
 Opens: C:\Windows\System32\version.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\mpr.dll  
 Opens: C:\Windows\System32\mpr.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp.Local\  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.ENU  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.ENU.DLL  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.EN  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.EN.DLL  
 Opens: C:\Windows\System32\rpcss.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\CRYPTBASE.dll  
 Opens: C:\Windows\System32\cryptbase.dll  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\dwmapi.dll  
 Opens: C:\Windows\Fonts\StaticCache.dat  
 Opens: C:\Windows\System32\en-US\user32.dll.mui  
 Opens: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\netmsg.dll  
 Opens: C:\Windows\Fonts\tahoma.ttf  
 Opens: C:\Windows\system32\uxtheme.dll.Config  
 Opens: C:\Windows\winsxs\x86\_microsoft.windows.c...-controls.resources\_6595b64144ccf1df\_6.0.7600.16385\_en-us\_581cd2bf5825dde9  
 Opens: C:\Windows\winsxs\x86\_microsoft.windows.c...-controls.resources\_6595b64144ccf1df\_6.0.7600.16385\_en-us\_581cd2bf5825dde9\comctl32.dll.mui  
 Writes to: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp  
 Reads from: C:\Windows\Temp\9605ec58da0d3fdca8679abd4c481cc3.exe  
 Reads from: C:\Users\Admin\AppData\Local\Temp\is-2D68R.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp  
 Reads from: C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

Opens key: HKLM\system\currentcontrolset\control\session manager  
 Opens key: HKLM\system\currentcontrolset\control\safeboot\option  
 Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll  
 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:  
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions  
 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\ole  
 Opens key: HKLM\software\microsoft\ole\tracing  
 Opens key: HKLM\software\microsoft\oleaut  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics  
 Opens key: HKCU\software\codegear\locales  
 Opens key: HKLM\software\codegear\locales  
 Opens key: HKCU\software\borland\locales  
 Opens key: HKCU\software\borland\delphi\locales  
 Opens key: HKLM\system\currentcontrolset\control\nls\customlocale  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr  
 Opens key: HKLM\system\currentcontrolset\control\cmf\config  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\9605ec58da0d3fdca8679abd4c481cc3.tmp  
 Opens key: HKLM\system\currentcontrolset\control\session manager\apppcertdlls  
 Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility  
 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\9605ec58da0d3fdca8679abd4c481cc3.tmp  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags  
 Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options  
 Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes  
 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\system\currentcontrolset\control\keyboard layouts\04090409  
 Opens key:  
 HKLM\software\microsoft\ctf\compatibility\9605ec58da0d3fdca8679abd4c481cc3.tmp  
 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\

Opens key: HKLM\software\microsoft\ctf\knownclasses  
 Opens key: HKLM\software\microsoft\windows  
 nt\currentversion\languagepack\surrogatefallback\tahoma  
 Opens key: HKCU\software\microsoft\windows\currentversion\uninstall\{da34b67a-29a4-4ac2-bac5-640c1327b3e4}\\_is1  
 Opens key: HKLM\software\microsoft\windows\currentversion\uninstall\{da34b67a-29a4-4ac2-bac5-640c1327b3e4}\\_is1  
 Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer  
 Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer  
 Queries value: HKLM\system\currentcontrolset\control\session  
 manager[cwdillegalindllsearch]  
 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: HKLM\system\currentcontrolset\control\nls\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\microsoft\windows  
 nt\currentversion\compatibility32[9605ec58da0d3fdca8679abd4c481cc3]  
 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\nls\customlocale[en-us]  
 Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]  
 Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]  
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]  
 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\layers[c:\users\admin\appdata\local\temp\is-2d68r.tmp\9605ec58da0d3fdca8679abd4c481cc3.tmp]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]  
 Queries value: HKCU\software\microsoft\windows  
 nt\currentversion\appcompatflags[{a9f603c2-b224-4a07-b6ea-a2bcc1a51297}]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]  
 Queries value: HKCU\software\microsoft\windows  
 nt\currentversion\appcompatflags[{6b39d1b2-7883-4648-94bf-bd5109b4ac48}]  
 Queries value: HKLM\software\microsoft\windows  
 nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]  
 Queries value: HKCU\software\microsoft\windows  
 nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options[disablelocaloverride]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms  
 shell dlg 2]  
 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]