

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 109, Task ID: 436

Task ID:	436
Risk Level:	1
Date Processed:	2016-04-28 12:58:57 (UTC)
Processing Time:	2.75 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8988ec168046b265016438a1fdf68d69.exe"
Sample ID:	109
Type:	basic
Owner:	admin
Label:	8988ec168046b265016438a1fdf68d69
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	28672 bytes
MD5:	8988ec168046b265016438a1fdf68d69
SHA256:	fde315967d49d286e48aecb4eb20cfad355c9fc8ef9a08aa387ab3042fe4811a
Description:	None

## Pattern Matching Results

### Static Events

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

### Process/Thread Events

Creates process:	C:\windows\temp\8988ec168046b265016438a1fdf68d69.exe
["C:\windows\temp\8988ec168046b265016438a1fdf68d69.exe" ]	
Terminates process:	C:\Windows\Temp\8988ec168046b265016438a1fdf68d69.exe

### Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?

8988EC168046B265016438A1FDF68D69.EXE

### File System Events

Opens:	C:\Windows\Prefetch\8988EC168046B265016438A1FDF68-CB9A5FCE.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\MSVBVM60.DLL
Opens:	C:\Windows\System32\msvbvm60.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\apphelp.dll
Opens:	C:\Windows\AppPatch\sysmain.sdb
Opens:	C:\Windows\Temp\8988ec168046b265016438a1fdf68d69.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\dwmapl.dll
Opens:	C:\Windows\System32\dwmapl.dll
Opens:	C:\windows\temp\MPR.dll
Opens:	C:\Windows\System32\mpr.dll
Opens:	C:\windows\temp\8988ec168046b265016438a1fdf68d69.exe.Manifest
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\System32\en-US\setupapi.dll.mui
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\windows\temp\8988ec168046b265016438a1fdf68d69.exe.cfg
Opens:	C:\windows\temp\SXS.DLL
Opens:	C:\Windows\System32\sxs.dll
Opens:	C:\Windows\System32\C_932.NLS
Opens:	C:\Windows\System32\C_949.NLS
Opens:	C:\Windows\System32\C_950.NLS
Opens:	C:\Windows\System32\C_936.NLS
Opens:	C:\Windows\WINHELP.INI
Opens:	C:\Windows\system32\HLP
Opens:	C:\Windows\Help\HLP

## 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\dl
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\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\dl\nxoptions
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\nls\customlocale  
 Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale  
 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\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\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: HKLM\system\currentcontrolset\control\nls\codepage  
 Opens key: HKLM\software\microsoft\vba\monitors  
 Opens key: HKLM\software\microsoft\windows  
 Opens key: HKLM\software\microsoft\windows\html help  
 Opens key: HKLM\software\microsoft\windows\help  
 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\microsoft\windows nt\currentversion\image file execution options\dlloptions[usefilter]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[msvbvm60.dll]  
 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[8988ec168046b265016438a1fdf68d69]  
 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\system\currentcontrolset\control\nls\locale[00000409]  
 Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]  
 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\services\crypt32[debugheapflags]  
 Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]  
 Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security\_hklm\_only]  
 Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]

Queries value:	HKLM\system\currentcontrolset\control\nls\codepage[932]
Queries value:	HKLM\system\currentcontrolset\control\nls\codepage[949]
Queries value:	HKLM\system\currentcontrolset\control\nls\codepage[950]
Queries value:	HKLM\system\currentcontrolset\control\nls\codepage[936]
Queries value:	HKLM\software\microsoft\windows\html help[.hlp]