

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 216, Task ID: 862

Task ID:	862
Risk Level:	1
Date Processed:	2016-04-28 13:11:24 (UTC)
Processing Time:	2.5 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\af08d8af6efe2bd3a801df9206306c08.exe"
Sample ID:	216
Type:	basic
Owner:	admin
Label:	af08d8af6efe2bd3a801df9206306c08
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	36864 bytes
MD5:	af08d8af6efe2bd3a801df9206306c08
SHA256:	4dd56d2ea589054858a876456ad1cb490c077fcd82590bbe72bf88ccf9885417
Description:	None

Pattern Matching Results

Static Events

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

Process/Thread Events

Creates process:	C:\windows\temp\af08d8af6efe2bd3a801df9206306c08.exe
["C:\windows\temp\af08d8af6efe2bd3a801df9206306c08.exe"]	
Terminates process:	C:\Windows\Temp\af08d8af6efe2bd3a801df9206306c08.exe

Named Object Events

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

AF08D8AF6EFE2BD3A801DF9206306C08.EXE

File System Events

Opens:	C:\Windows\Prefetch\AF08D8AF6EFE2BD3A801DF9206306-6B194200.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\af08d8af6efe2bd3a801df9206306c08.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\SysWOW64\msvbvm60.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.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\advapi32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\Windows\SysWOW64\sxs.dll
Opens:	C:\Windows\SysWOW64\clbcatq.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\Windows\WINHELP.INI

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\srb\gp\ddl
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\system\currentcontrolset\control\session manager
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\dlxnoptions	
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\software\wow6432node\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
 Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
 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\wow6432node\microsoft\windows\windows error reporting\wmr
 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\system\currentcontrolset\control\nls\codepage
 Opens key: HKLM\software\wow6432node\microsoft\vba\monitors
 Opens key: HKCU\software\classes\
 Opens key: HKLM\software\microsoft\com3
 Opens key: HKLM\software\microsoft\windowsruntime\clsid
 Opens key: HKLM\software\microsoft\windowsruntime\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKCR\activatableclasses\clsid
 Opens key: HKCR\activatableclasses\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKCU\software\classes\wow6432node\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKCR\wow6432node\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKCU\software\classes\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKCR\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKCU\software\classes\activatableclasses\clsid
 Opens key: HKCU\software\classes\activatableclasses\clsid\{8e60279e-2787-4e7d-8414-08e12198c34b}
 Opens key: HKLM\software\wow6432node\microsoft\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\setup
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKCU\software\classes\appid\af08d8af6efe2bd3a801df9206306c08.exe
 Opens key: HKCR\appid\af08d8af6efe2bd3a801df9206306c08.exe
 Opens key: HKLM\software\wow6432node\microsoft\ole\appcompat
 Opens key: HKLM\software\microsoft\ole\appcompat
 HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider
 Opens key: HKLM\software\policies\microsoft\cryptography
 Opens key: HKLM\software\microsoft\cryptography
 Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload
 Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
 Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}
 Opens key: HKCU\software\classes\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
 Opens key: HKCR\wow6432node\interface\{00000134-0000-0000-c000-000000000046}\proxystubclsid32
 Opens key: HKLM\software\wow6432node\microsoft\rpc\extensions
 Opens key: HKLM\software\microsoft\rpc\extensions
 Opens key: HKCU\software\policies\microsoft\windows\app management
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\app management
 Opens key: HKLM\software\policies\microsoft\windows\app management
 Opens key: HKLM\software\wow6432node\microsoft\windows
 Opens key: HKLM\software\wow6432node\microsoft\windows\html help
 Opens key: HKLM\software\wow6432node\microsoft\windows\help
 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\microsoft\windows nt\currentversion\image file execution options\dllexoptions[usefilter]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllexoptions[msvbvm60.dll]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllexoptions[af08d8af6efe2bd3a801df9206306c08.exe]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[af08d8af6efe2bd3a801df9206306c08]
 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[pageallocatorssystemheapisprivate]
 Queries value: HKLM\software\microsoft\ole[aggressivemtesting]
 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\system\currentcontrolset\control\nls\locale[00000409]
 Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
 Queries value: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]
 Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
 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\com3[com+enabled]
 Queries value: HKLM\software\microsoft\ole[maxsxshashcount]
 Queries value: HKLM\software\microsoft\rpc[maxrpcsize]
 Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]
 Queries value: HKLM\system\setup[oobeinprogress]
 Queries value: HKLM\system\setup[systemsetupinprogress]
 Queries value: HKLM\software\microsoft\rpc[idletimerwindow]
 Queries value: HKLM\software\microsoft\ole\appcompat[raisedefaultauthnlevel]
 Queries value: HKLM\software\microsoft\ole[defaultaccesspermission]
 Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]
 Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[type]
 Queries value: HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic provider[image path]
 Queries value: HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]
 Queries value:

HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]
Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]
Queries value: HKLM\software\microsoft\cryptography[machineguid]
Queries value: HKCR\wow6432node\interface\{00000134-0000-0000-c000-
000000000046}\proxystubclsid32[]
Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\wow6432node\microsoft\windows\html help[.hlp]