

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 15, Task ID: 57

Task ID:	57
Risk Level:	1
Date Processed:	2016-04-28 12:47:37 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7ab9ac3f6065eae2e29fcbacd2d8cdb9.exe"
Sample ID:	15
Type:	basic
Owner:	admin
Label:	7ab9ac3f6065eae2e29fcbacd2d8cdb9
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	278528 bytes
MD5:	7ab9ac3f6065eae2e29fcbacd2d8cdb9
SHA256:	94c8f7271d904be7da91d86c12d23183d6643858ee06beea9c5e834e51b1735a
Description:	None

## Pattern Matching Results

1	YARA score 1
---	--------------

## Static Events

YARA rule hit:	OLE2
YARA rule hit:	Nonexecutable

## Process/Thread Events

Creates process:	C:\windows\temp\7ab9ac3f6065eae2e29fcbacd2d8cdb9.exe
["C:\windows\temp\7ab9ac3f6065eae2e29fcbacd2d8cdb9.exe" ]	

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates event:	\Sessions\1\BaseNamedObjects\OleDfRootC757F2C6DFC42507
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?
7AB9AC3F6065EAE2E29FCBACD2D8CDB9.EXE	

## File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\~DFA74F507C74054875.TMP
Opens:	C:\Windows\Prefetch\7AB9AC3F6065EAE2E29FCBACD2D8C-E956FA41.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\7ab9ac3f6065eae2e29fcbacd2d8cdb9.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\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\Fonts\sserife.fon
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\Windows\SysWOW64\dwmapl.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Reads from:	C:\Windows\Fonts\StaticCache.dat

Windows Registry Events

Creates key:	HKCU\software\vb and vba program settings\ultimate startup
manager\presets	
Creates key:	HKCU\software
Creates key:	HKCU\software\vb and vba program settings
Creates key:	HKCU\software\vb and vba program settings\ultimate startup manager
Creates key:	HKCU\software\vb and vba program settings\ultimate startup
manager\logged	
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\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\dllnsoptions	
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\lipsalgorithmpolicy  
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\{c82a6835-26d9-11d7-9049-  
00a0cc59f8af}  
Opens key: HKCR\activatableclasses\clsid  
Opens key: HKCR\activatableclasses\clsid\{c82a6835-26d9-11d7-9049-00a0cc59f8af}  
Opens key: HKCU\software\classes\wow6432node\clsid\{c82a6835-26d9-11d7-9049-  
00a0cc59f8af}  
Opens key: HKCR\wow6432node\clsid\{c82a6835-26d9-11d7-9049-00a0cc59f8af}  
Opens key: HKCU\software\classes\clsid\{c82a6835-26d9-11d7-9049-00a0cc59f8af}  
Opens key: HKCR\clsid\{c82a6835-26d9-11d7-9049-00a0cc59f8af}  
Opens key: HKCU\software\classes\activatableclasses\clsid  
Opens key: HKCU\software\classes\activatableclasses\clsid\{c82a6835-26d9-11d7-9049-  
00a0cc59f8af}  
Opens key: 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: HKLM\software\wow6432node\microsoft\ctf\compatibility\7ab9ac3f6065eae2e29fcbacd2d8cdb9.exe

Opens key: HKCU\software\vba and vba program settings\ultimate startup  
manager\presets

Opens key: HKLM\software\wow6432node\microsoft\oleaut\userera  
Opens key: HKCU\software\policies\microsoft\control

panel\international\calendars\twodigityearmax  
Opens key: HKCU\control panel\international\calendars\twodigityearmax  
Opens key: HKLM\software\wow6432node\microsoft\ctf\  
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses  
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\ms sans serif  
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\dlloptions[usefilter]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[msvbvm60.dll]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloptions[7ab9ac3f6065eae2e29fcbacd2d8cdb9.exe]  
 Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]  
 Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[7ab9ac3f6065eae2e29fcbacd2d8cdb9]  
 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[aggressivemtatesting]  
 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\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: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]  
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]  
Sets/Creates value: HKCU\software\vb and vba program settings\ultimate startup  
manager\presets[serial]  
Sets/Creates value: HKCU\software\vb and vba program settings\ultimate startup  
manager\presets[postop]  
Sets/Creates value: HKCU\software\vb and vba program settings\ultimate startup  
manager\presets[posleft]  
Sets/Creates value: HKCU\software\vb and vba program settings\ultimate startup  
manager\logged[expired]