

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 217, Task ID: 868

Task ID:	868
Risk Level:	4
Date Processed:	2016-04-28 13:11:38 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe"
Sample ID:	217
Type:	basic
Owner:	admin
Label:	af7d9dfcdc5262aea00f7c8ed6e0adff
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	961320 bytes
MD5:	af7d9dfcdc5262aea00f7c8ed6e0adff
SHA256:	611a9496aef3dd7edfcf734651f2cc8c77d01b6f0f584f63d60d7b5191df0ecc
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe
["C:\windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe" ]	

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfdMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfdActivated.Default1

## File System Events

Opens:	C:\Windows\Prefetch\AF7D9DFCDC5262AEA00F7C8ED6E0A-BF95386E.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\temp\af7d9dfcdc5262aea00f7c8ed6e0adff.exe.Local\
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens:	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
Opens:	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
Opens:	C:\windows\temp\VERSION.dll
Opens:	C:\Windows\System32\version.dll
Opens:	C:\windows\temp\pdh.dll
Opens:	C:\Windows\System32\pdh.dll
Opens:	C:\windows\temp\WTSAPI32.dll
Opens:	C:\Windows\System32\wtsapi32.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\Windows\System32\en-US\user32.dll.mui
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
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\ddl  
 Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers  
 Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers  
 Opens key:  
 HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 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\system\currentcontrolset\control\nls\sorting\versions  
 Opens key: HKLM\  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics  
 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\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\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\software\microsoft\windows nt\currentversion\pdh  
 Opens key: HKLM\software\microsoft\rpc  
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername  
 Opens key: HKLM\system\setup  
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc  
 Opens key: HKLM\software\policies\microsoft\sqmclient\windows  
 Opens key: HKLM\software\microsoft\sqmclient\windows  
 Opens key: HKLM\system\currentcontrolset\control\computername  
 Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr  
 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\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\cmf\config  
 Opens key:  
 HKLM\software\microsoft\ctf\compatibility\af7d9dfcdc5262aea00f7c8ed6e0adff.exe  
 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\  
 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[af7d9dfcdc5262aea00f7c8ed6e0adff]  
 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\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\software\microsoft\rpc[maxrpcsize]
  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\sqmclient\windows[ceipenable]
  Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  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]
  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\system\currentcontrolset\control\cmf\config[system]
  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]
```