

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 20, Task ID: 80

Task ID:	80
Risk Level:	4
Date Processed:	2016-04-28 12:48:47 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\80fbf80dc58b4ccaebf7fc36947ab18b.exe"
Sample ID:	20
Type:	basic
Owner:	admin
Label:	80fbf80dc58b4ccaebf7fc36947ab18b
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	217600 bytes
MD5:	80fbf80dc58b4ccaebf7fc36947ab18b
SHA256:	b29002f77b078e0db2d5433ca0579927aaabec579f69b5f748cee63b0e443158
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\windows\temp\80fbf80dc58b4ccaebf7fc36947ab18b.exe
["C:\windows\temp\80fbf80dc58b4ccaebf7fc36947ab18b.exe" ]	

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfnMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfnActivated.Default1

## File System Events

Opens:	C:\Windows\Prefetch\80FBF80DC58B4CCAEBF7FC36947AB-E46E934F.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\windows\temp\80fbf80dc58b4ccaebf7fc36947ab18b.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\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742
Opens:	C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcr90.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\
Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\rpcss.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\uxtheme.dll.Config

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\WindowsShell.Manifest  
Reads from: C:\Windows\Fonts\StaticCache.dat

## Windows Registry Events

---

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options  
Opens key: HKLM\system\currentcontrolset\control\session manager  
Opens key: HKLM\software\microsoft\wow64  
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options  
Opens key: HKLM\system\currentcontrolset\control\safeboot\option  
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dl  
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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions  
Opens key: HKLM\  
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics  
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\software\wow6432node\microsoft\windows nt\currentversion\windows  
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\wow6432node\microsoft\ctf\compatibility\80fbf80dc58b4ccaebf7fc36947ab18b.exe  
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\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}

Opens key: HKLM\software\wow6432node\microsoft\ctf\

Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses

Opens key:

HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer

Opens key: HKLM\software\microsoft\windows\currentversion\policies\explorer

Opens key: HKCU\software\microsoft\windows\currentversion\policies\explorer

Opens key: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback\system

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]

Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]

Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKLM\system\currentcontrolset\control\ntp\customlocale[empty]

Queries value:

HKLM\system\currentcontrolset\control\ntp\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\ntp\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\wow6432node\microsoft\windows

nt\currentversion\compatibility32[80fbf80dc58b4ccaebf7fc36947ab18b]

Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\windows[loadappinit\_dlls]

Queries value: HKLM\system\currentcontrolset\control\ntp\customlocale[en-us]

Queries value: HKLM\system\currentcontrolset\control\ntp\extendedlocale[en-us]

Queries value: HKLM\system\currentcontrolset\control\ntp\locale[00000409]

Queries value: HKLM\system\currentcontrolset\control\ntp\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\system\currentcontrolset\control\cmf\config[system]  
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]  
Queries value: HKLM\software\microsoft\ole[pageallocatorssystemheapisprivate]  
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-  
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]  
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]  
Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]