

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 100, Task ID: 401

Task ID:	401
Risk Level:	1
Date Processed:	2016-04-28 12:57:48 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\006bfb7286f8b1511346975a4ec7d3d4.exe"
Sample ID:	100
Type:	basic
Owner:	admin
Label:	006bfb7286f8b1511346975a4ec7d3d4
Date Added:	2016-04-28 12:45:00 (UTC)
File Type:	PE32:win32:gui
File Size:	114688 bytes
MD5:	006bfb7286f8b1511346975a4ec7d3d4
SHA256:	bbd9d3e1421fede3b6dc485ef528181204dfa5959105875782b0f79978d847b9
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\006bfb7286f8b1511346975a4ec7d3d4.exe
["C:\windows\temp\006bfb7286f8b1511346975a4ec7d3d4.exe" ]	

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex:	\Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event:	\Sessions\1\BaseNamedObjects\OleDfRootCAB532EA9A254BBE
Creates event:	\KernelObjects\MaximumCommitCondition
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1
Creates semaphore:	\Sessions\1\BaseNamedObjects\C:?WINDOWS?TEMP?
006BFB7286F8B1511346975A4EC7D3D4.EXE	

## File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\~DF738F2C3DFE90B547.TMP
Opens:	C:\Windows\Prefetch\006BFB7286F8B1511346975A4EC7D-3B714260.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\temp\MSVBVM60.DLL
Opens:	C:\Windows\SysWOW64\msvbvm60.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:	C:\Windows\SysWOW64\rpcss.dll

Opens:	C:\Windows\SysWOW64\uxtheme.dll
Opens:	C:\windows\temp\006bfb7286f8b1511346975a4ec7d3d4.exe.cfg
Opens:	C:\windows\temp\SXS.DLL
Opens:	C:\Windows\SysWOW64\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\SysWOW64\VB6DE.DLL
Opens:	C:\Windows\Fonts\sserife.fon
Opens:	C:\Windows\SysWOW64\asycfilt.dll
Opens:	C:\windows\temp\CRYPTSP.dll
Opens:	C:\Windows\SysWOW64\cryptsp.dll
Opens:	C:\Windows\SysWOW64\rsaenh.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\SysWOW64\dwmapi.dll
Opens:	C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens:	C:\Windows\SysWOW64\uxtheme.dll.Config
Opens:	C:\windows\temp\006bfb7286f8b1511346975a4ec7d3d4.exe.Local\
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
Opens:	C:\windows\temp\COMDLG32.OCX
Opens:	C:\Windows\SysWOW64\COMDLG32.OCX
Opens:	C:\Windows\system\COMDLG32.OCX
Opens:	C:\Windows\COMDLG32.OCX
Opens:	C:\Windows\SysWOW64\Wbem\COMDLG32.OCX
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\COMDLG32.OCX
Opens:	C:\Windows\Fonts\StaticCache.dat
Opens:	C:\Windows\SysWOW64\ole32.dll
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\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\  
 Opens key: HKLM\software\wow6432node\microsoft\windows  
 nt\currentversion\diagnostics  
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution  
 options\dlloptions  
 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\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\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\system\currentcontrolset\control\nls\codepage  
 Opens key: HKLM\software\wow6432node\microsoft\vba\monitors  
 Opens key:  
 HKLM\software\wow6432node\microsoft\cryptography\defaults\provider\microsoft strong cryptographic  
 provider  
 Opens key: HKLM\system\currentcontrolset\control\lsa\lspolicy  
 Opens key: HKLM\system\currentcontrolset\control\lsa  
 Opens key:  
 HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration  
 Opens key: HKLM\software\policies\microsoft\cryptography  
 Opens key: HKLM\software\microsoft\cryptography  
 Opens key: HKLM\software\wow6432node\microsoft\cryptography\offload  
 Opens key: HKLM\system\currentcontrolset\control\cmf\config  
 Opens key:  
 HKLM\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots  
 Opens key:  
 HKLM\software\wow6432node\microsoft\ctf\compatibility\006bfb7286f8b1511346975a4ec7d3d4.exe  
 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: HKCU\software\classes\  
 Opens key: HKLM\software\microsoft\com3  
 Opens key: HKCU\software\classes\wow6432node\clsid\{f9043c85-f6f2-101a-a3c9-  
 08002b2f49fb}  
 Opens key: HKCR\wow6432node\clsid\{f9043c85-f6f2-101a-a3c9-08002b2f49fb}  
 Opens key: HKCU\software\classes\clsid\{f9043c85-f6f2-101a-a3c9-08002b2f49fb}  
 Opens key: HKCR\clsid\{f9043c85-f6f2-101a-a3c9-08002b2f49fb}  
 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\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\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\

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\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[alternatencodepage]

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: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

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

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dlloxoptions[msvbvm60.dll]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre\_initialize[disablemetafiles]

Queries value: HKLM\software\wow6432node\microsoft\windows nt\currentversion\compatibility32[006bfb7286f8b1511346975a4ec7d3d4]

Queries value: HKLM\software\wow6432node\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\software\wow6432node\microsoft\windows\windows error reporting\wmr[disable]

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\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\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]

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\system\currentcontrolset\control\cmf\config[system]

Queries value: HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]  
Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]  
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\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]