

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 87, Task ID: 346

Task ID:	346
Risk Level:	4
Date Processed:	2016-04-28 12:56:35 (UTC)
Processing Time:	3.26 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe"
Sample ID:	87
Type:	basic
Owner:	admin
Label:	9051f3a2023c56661804fd664e27c74c
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	312320 bytes
MD5:	9051f3a2023c56661804fd664e27c74c
SHA256:	8ac177e931c1a04d468ba07162f5acdf48cbb1e1351afbbbf6ca99dac795e079
Description:	None

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process:	C:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe
["C:\windows\temp\9051f3a2023c56661804fd664e27c74c.exe" ]	
Terminates process:	C:\Windows\Temp\9051f3a2023c56661804fd664e27c74c.exe

## Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
----------------	---

## File System Events

Opens:	C:\Windows\Prefetch\9051F3A2023C56661804FD664E27C-FC80E9F4.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\9051f3a2023c56661804fd664e27c74c.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\IPHLAPI.DLL
Opens:	C:\Windows\SysWOW64\msvcp100.dll
Opens:	C:\Windows\SysWOW64\msvcr100.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\winhttp.dll
Opens:	C:\Windows\SysWOW64\winnsi.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\nsi.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\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.dll

Opens:	C:\Windows\SysWOW64\msvcrt.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\SysWOW64\shlwapi.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll

## Windows Registry Events

---

Opens key:	HKLM\software\microsoft\wow64
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\ntp\customlocale
Opens key:	HKLM\system\currentcontrolset\control\ntp\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\ntp\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\system\currentcontrolset\control\lsa\lspalgorithm\policy
Opens key:	HKLM\system\currentcontrolset\control\lsa
Opens key:	
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration	
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\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\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key:	HKCU\software\classes\
Opens key:	HKCU\software\classes\appid
Opens key:	HKCR\appid
Opens key:	HKCU\software\classes\appid\{068808b5-8e5c-463b-97ec-548be3668d1d}
Opens key:	HKCR\appid\{068808b5-8e5c-463b-97ec-548be3668d1d}
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\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\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]  
Queries value: HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]  
Queries value: HKLM\software\microsoft\windows  
nt\currentversion\gre\_initialize[disablemetafiles]  
Queries value: HKLM\software\wow6432node\microsoft\windows  
nt\currentversion\compatibility32[9051f3a2023c56661804fd664e27c74c]  
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\software\microsoft\ole[aggressivemtatesting]  
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error  
reporting\wmr[disable]