

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 79, Task ID: 314

Task ID:	314
Risk Level:	4
Date Processed:	2016-04-28 12:55:56 (UTC)
Processing Time:	2.2 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8f86b1cb567c6b56537468c70bc3c08b.exe"
Sample ID:	79
Type:	basic
Owner:	admin
Label:	8f86b1cb567c6b56537468c70bc3c08b
Date Added:	2016-04-28 12:44:58 (UTC)
File Type:	PE32:win32:gui
File Size:	117656 bytes
MD5:	8f86b1cb567c6b56537468c70bc3c08b
SHA256:	c14bcd99b2dfee2b05be8f37e80e8f7604ca83d350fa69befb9a6b41bc8f4e0
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\8f86b1cb567c6b56537468c70bc3c08b.exe
["C:\windows\temp\8f86b1cb567c6b56537468c70bc3c08b.exe"]	
Terminates process:	C:\Windows\Temp\8f86b1cb567c6b56537468c70bc3c08b.exe

Named Object Events

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

File System Events

Opens:	C:\Windows\Prefetch\8F86B1CB567C6B56537468C70BC3C-11B10CF0.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\8f86b1cb567c6b56537468c70bc3c08b.exe
Opens:	C:\Windows\SysWOW64\ntdll.dll
Opens:	C:\Windows\SysWOW64\kernel32.dll
Opens:	C:\Windows\SysWOW64\KernelBase.dll
Opens:	C:\Windows\apppatch\sysmain.sdb
Opens:	C:\Windows\SysWOW64\version.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\shlwapi.dll
Opens:	C:\Windows\SysWOW64\shell32.dll
Opens:	C:\Windows\SysWOW64\ole32.dll
Opens:	C:\Windows\SysWOW64\msasn1.dll

Opens:	C:\Windows\SysWOW64\crypt32.dll
Opens:	C:\Windows\SysWOW64\wintrust.dll
Opens:	C:\Windows\SysWOW64\imm32.dll
Opens:	C:\Windows\SysWOW64\msctf.dll
Opens:	C:\Windows\SysWOW64\oleaut32.dll
Opens:	C:\Windows\Globalization\Sorting\SortDefault.nls

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\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\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\fipsalgorithmpolicy
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\system\currentcontrolset\services\crypt32
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
Opens key:	HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\ids
Opens key:	HKLM\software\wow6432node\microsoft\rpc
Opens key:	HKLM\system\currentcontrolset\control\computername\activecomputername
Opens key:	HKLM\system\setup
Opens key:	HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
Opens key:	HKLM\software\policies\microsoft\windows nt\rpc
Opens key:	HKLM\software\policies\microsoft\sqmclient\windows
Opens key:	HKLM\software\microsoft\sqmclient\windows
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\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\wow6432node\microsoft\windows

nt\currentversion\compatibility32[8f86b1cb567c6b56537468c70bc3c08b]
 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\services\crypt32[debugheapflags]
 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\software\microsoft\rpc[maxrpcsize]
 Queries 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\rpc[idletimerwindow]