

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 78, Task ID: 311

Task ID:	311
Risk Level:	4
Date Processed:	2016-04-28 12:55:54 (UTC)
Processing Time:	17.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\cabce7b103edbf8de78e66e8502ff79a.exe"
Sample ID:	78
Type:	basic
Owner:	admin
Label:	cabce7b103edbf8de78e66e8502ff79a
Date Added:	2016-04-28 12:44:57 (UTC)
File Type:	PE32:win32:gui
File Size:	118696 bytes
MD5:	cabce7b103edbf8de78e66e8502ff79a
SHA256:	49455b80663800dbfae31333fb12ef3e21431348215fb2ef6ec0a650ab800da1
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\cabce7b103edbf8de78e66e8502ff79a.exe
["c:\windows\temp\cabce7b103edbf8de78e66e8502ff79a.exe"]	
Terminates process:	C:\WINDOWS\Temp\cabce7b103edbf8de78e66e8502ff79a.exe

Named Object Events

Creates semaphore:	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
--------------------	--

File System Events

Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\wintrust.dll
Opens:	C:\WINDOWS\system32\crypt32.dll
Opens:	C:\WINDOWS\system32\msasn1.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\shell32.dll
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\SHELL32.dll.124.Config
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\WindowsShell.Manifest
Opens:	C:\WINDOWS\WindowsShell.Config
Opens:	C:\WINDOWS\system32\comctl32.dll
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Manifest
Opens:	C:\WINDOWS\system32\comctl32.dll.124.Config

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\cabce7b103edbf8de78e66e8502ff79a.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers

Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\gdi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\user32.dll	
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imm32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ntdll.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\kernel32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\secur32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\rpcrt4.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\advapi32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvcrt.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shlwapi.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\shell32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msasn1.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\crypt32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\imagehlp.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\wintrust.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\ole32.dll	
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\windows nt\currentversion\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key:	HKLM\software\microsoft\windows\currentversion\explorer\performance
Opens key:	HKLM\system\setup
Opens key:	HKCU\
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop
Opens key:	
HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\comctl32.dll	
Opens key:	HKCU\software\microsoft\windows\currentversion\explorer\advanced
Opens key:	HKLM\software\microsoft\windows nt\currentversion\languagepack
Opens key:	HKLM\system\currentcontrolset\services\crypt32\performance
Opens key:	HKLM\software\microsoft\windows nt\currentversion\msasn1
Opens key:	HKLM\software\microsoft\ole
Opens key:	HKCR\interface
Opens key:	HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key:	HKLM\system\currentcontrolset\control\servicecurrent
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]

Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
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[cabce7b103edbf8de78e66e8502ff79a]
Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
compatibility[cabce7b103edbf8de78e66e8502ff79a]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
Queries value: HKLM\system\setup[systemsetupinprogress]
Queries value: HKCU\control panel\desktop[multiuilanguageid]
Queries value: HKCU\control panel\desktop[smoothscroll]
Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
Queries value: HKLM\system\currentcontrolset\control\session
manager[criticalsectiontimeout]
Queries value: HKLM\software\microsoft\ole[rwlockresourcetimeout]
Queries value: HKCR\interface[interfacehelperdisableall]
Queries value: HKCR\interface[interfacehelperdisableallforole32]
Queries value: HKCR\interface[interfacehelperdisabletypelib]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableall]
Queries value: HKCR\interface\{00020400-0000-0000-c000-
000000000046}[interfacehelperdisableallforole32]
Queries value: HKLM\system\currentcontrolset\control\servicecurrent[]
Value changes: HKLM\software\microsoft\cryptography\rng[seed]