

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 109, Task ID: 435

Task ID:	435
Risk Level:	1
Date Processed:	2016-04-28 12:58:48 (UTC)
Processing Time:	2.19 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8988ec168046b265016438a1fdf68d69.exe"
Sample ID:	109
Type:	basic
Owner:	admin
Label:	8988ec168046b265016438a1fdf68d69
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	28672 bytes
MD5:	8988ec168046b265016438a1fdf68d69
SHA256:	fde315967d49d286e48aecb4eb20cfad355c9fc8ef9a08aa387ab3042fe4811a
Description:	None

Pattern Matching Results

Static Events

Anomaly:	PE: Contains a virtual section
----------	--------------------------------

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\8988ec168046b265016438a1fdf68d69.exe
["c:\windows\temp\8988ec168046b265016438a1fdf68d69.exe"]	
Terminates process:	C:\WINDOWS\Temp\8988ec168046b265016438a1fdf68d69.exe

Named Object Events

Creates mutex:	\BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates semaphore:	\BaseNamedObjects\C:?WINDOWS?TEMP?8988EC168046B265016438A1FDF68D69.EXE

File System Events

Opens:	C:\WINDOWS\Prefetch\8988EC168046B265016438A1FDF68-09CE54AA.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\msvbvm60.dll
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\system32\rpcss.dll
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\sxs.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\WINHELP.INI

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\8988ec168046b265016438a1fdf68d69.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\ole32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\oleaut32.dll	
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msvbvm60.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\ole
Opens key:	HKCR\interface
Opens key:	HKCR\interface\{00020400-0000-0000-c000-000000000046}
Opens key:	HKLM\software\microsoft\oleaut
Opens key:	HKLM\software\microsoft\oleaut\userera
Opens key:	HKCU\
Opens key:	HKCU\software\policies\microsoft\control panel\desktop
Opens key:	HKCU\control panel\desktop
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\msctf.dll	
Opens key:	
HKLM\software\microsoft\ctf\compatibility\8988ec168046b265016438a1fdf68d69.exe	
Opens key:	HKLM\software\microsoft\ctf\systemshared\
Opens key:	HKCU\keyboard layout\toggle
Opens key:	HKLM\software\microsoft\ctf\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\sxs.dll	
Opens key:	HKLM\system\setup
Opens key:	HKLM\software\microsoft\windows nt\currentversion\imm
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution
options\version.dll	

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\msctfime.ime
 Opens key: HKCU\software\microsoft\ctf
 Opens key: HKLM\software\microsoft\ctf\systemshared
 Opens key: HKLM\system\currentcontrolset\control\nls\codepage
 Opens key: HKLM\software\microsoft\vba\monitors
 Opens key: HKLM\software\microsoft\windows
 Opens key: HKLM\software\microsoft\windows\html help
 Opens key: HKLM\software\microsoft\windows\help
 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[8988ec168046b265016438a1fdf68d69]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[8988ec168046b265016438a1fdf68d69]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 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: HKCU\control panel\desktop[multiuilanguageid]
 Queries value: HKLM\software\microsoft\ctf\systemshared[cuas]
 Queries value: HKCU\keyboard layout\toggle[language hotkey]
 Queries value: HKCU\keyboard layout\toggle[hotkey]
 Queries value: HKCU\keyboard layout\toggle[layout hotkey]
 Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[safeprocesssearchmode]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\imm[ime file]
 Queries value: HKCU\software\microsoft\ctf[disable thread input manager]
 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]
 Value changes: HKLM\software\microsoft\cryptography\rng[seed]