

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 235, Task ID: 939

Task ID:	939
Risk Level:	5
Date Processed:	2016-04-28 13:13:18 (UTC)
Processing Time:	61.3 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\f606c36e9591fbfd0d5f15ddfb01864b.exe"
Sample ID:	235
Type:	basic
Owner:	admin
Label:	f606c36e9591fbfd0d5f15ddfb01864b
Date Added:	2016-04-28 12:45:14 (UTC)
File Type:	PE32:win32:gui
File Size:	381440 bytes
MD5:	f606c36e9591fbfd0d5f15ddfb01864b
SHA256:	33ccd74ddd83ea4a3e279b6653897da0298c08fd79df4cbc93375b8a57ef1468
Description:	None

Pattern Matching Results

5 PE: Contains compressed section

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\f606c36e9591fbfd0d5f15ddfb01864b.exe
["c:\windows\temp\f606c36e9591fbfd0d5f15ddfb01864b.exe"]	
Creates process:	C:\WINDOWS\Temp\sxe3.tmp ["c:\windows\temp\sxe3.tmp"]

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 mutex:	MUTEX.DefaultS-1-5-21-1757981266-507921405-1957994488-1003
Creates mutex:	\BaseNamedObjects\MSCTF.Shared.MUTEX.AGH

File System Events

Creates:	C:\WINDOWS\Temp\sxe1.tmp
Creates:	C:\WINDOWS\Temp\sxe2.tmp
Creates:	C:\WINDOWS\Temp\sxe3.tmp
Opens:	C:\WINDOWS\Prefetch\F606C36E9591FBFD0D5F15DDFB018-11981CF2.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\system32\imm32.dll
Opens:	C:\WINDOWS\Temp\0e1816c9-a5bf-4c9f-aebd-48a72a4adeec
Opens:	C:\WINDOWS\Temp
Opens:	C:\WINDOWS\Temp\sxe2.tmp
Opens:	C:\WINDOWS\Temp\sxe1.tmp
Opens:	C:\WINDOWS\Temp\sxe3.tmp
Opens:	C:\WINDOWS\system32\apphelp.dll
Opens:	C:\WINDOWS\AppPatch\sysmain.sdb

Opens:	C:\WINDOWS\AppPatch\sysrest.sdb
Opens:	C:\
Opens:	C:\WINDOWS
Opens:	C:\windows\temp\sxe3.tmp.Manifest
Opens:	C:\WINDOWS\Prefetch\SXE3.TMP-106AA75F.pf
Opens:	C:\WINDOWS\Fonts\sserife.fon
Opens:	C:\WINDOWS\system32\MSCTF.dll
Opens:	C:\WINDOWS\system32\MSCTFIME.IME
Opens:	C:\WINDOWS\system32\ole32.dll
Writes to:	C:\WINDOWS\Temp\sxe2.tmp
Writes to:	C:\WINDOWS\Temp\sxe1.tmp
Writes to:	C:\WINDOWS\Temp\sxe3.tmp
Reads from:	C:\WINDOWS\Temp\sxe2.tmp
Deletes:	C:\WINDOWS\Temp\sxe2.tmp
Deletes:	C:\WINDOWS\Temp\sxe1.tmp

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\fb06c36e9591fbfd0d5f15ddfb01864b.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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\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\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\winlogon
Opens key:	HKLM\
Opens key:	HKLM\software\microsoft\windows nt\currentversion\diagnostics
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\lz32.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:	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\sxe1.tmp
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key:	HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\apphelp.dll
Opens key:	HKLM\system\wpa\tabletpc
Opens key:	HKLM\system\wpa\mediacenter
Opens key:	HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers
Opens key: HKLM\software\microsoft\windows
nt\currentversion\appcompatflags\custom\sxe3.tmp
Opens key: HKLM\software\policies\microsoft\windows\safer\levelobjects
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddec3f}
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
Opens key:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\paths
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\0\urlzones
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\paths
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\hashes
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\4096\urlzones
Opens key:
HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\paths
Opens key:

HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\65536\urlzones
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\paths
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\131072\urlzones
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\paths
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\hashes
 Opens key:
 HKCU\software\policies\microsoft\windows\safer\codeidentifiers\262144\urlzones
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\sxe3.tmp
 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\msctf.dll
 Opens key: HKLM\software\microsoft\ctf\compatibility\sxe3.tmp
 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\imm
 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\msctfime.ime
 Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
 options\ole32.dll
 Opens key: HKLM\software\microsoft\ole
 Opens key: HKCR\interface
 Opens key: HKCR\interface\{00020400-0000-0000-c000-000000000046}
 Opens key: HKCU\software\microsoft\ctf
 Opens key: HKLM\software\microsoft\ctf\systemshared
 Opens key: HKCU\software\microsoft\ctf\langbaraddin\
 Opens key: HKLM\software\microsoft\ctf\langbaraddin\
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
 Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
 Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\winlogon[leaktrack]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\gre_initialize[disablemetafiles]
 Queries value: HKLM\software\microsoft\windows
 nt\currentversion\compatibility32[f606c36e9591fbfd0d5f15ddfb01864b]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[f606c36e9591fbfd0d5f15ddfb01864b]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[appinit_dlls]
 Queries value: HKCU\control panel\desktop[multiuilanguageid]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager[safeprocesssearchmode]
 Queries value: HKLM\system\currentcontrolset\control\session
 manager\appcompatibility[disableappcompat]
 Queries value: HKLM\system\wpa\mediacenter[installed]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
 Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[levels]
 Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\paths\{dda3f824-d8cb-441b-834d-be2efd2c1a33}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[itemsizedata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{349d35ab-37b5-462f-9b89-edd5fbde1328}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[itemsizedata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{7fb9cd2e-3076-4df9-a57b-b813f72dbb91}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[itemsizedata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{81d1fe15-dd9d-4762-b16d-7c29ddecae3f}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[itemsizedata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{94e3e076-8f53-42a5-8411-085bcc18a68d}[saferflags]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemdata]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[hashalg]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[itemsizedata]
Queries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers\0\hashes\{dc971ee5-44eb-4fe4-ae2e-b91490411bfc}[saferflags]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[defaultlevel]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[policyscope]
 Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell
 folders[cache]
 Queries value:
 HKLM\software\policies\microsoft\windows\safer\codeidentifiers[logfilename]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[sxe3]
 Queries value: HKLM\software\microsoft\windows nt\currentversion\ime
 compatibility[sxe3]
 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\software\microsoft\windows nt\currentversion\imm[ime file]
 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\software\microsoft\ctf[disable thread input manager]
 Value changes: HKLM\software\microsoft\cryptography\rng[seed]