Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 235, Task ID: 940

Task ID:	940
Risk Level:	5
Date Processed:	2016-04-28 13:13:18 (UTC)
Processing Time:	61.16 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\sxeB729.tmp ["C:\windows\temp\sxeB729.tmp"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates: C:\Windows\Temp\sxeB71D.tmp
Creates: C:\Windows\Temp\sxeB71E.tmp
Creates: C:\Windows\Temp\sxeB729.tmp
Opens: C:\Windows\Prefetch\F606C36E9591FBFD0D5F15DDFB018-C8675F27.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\LZ32.dll
Opens: C:\Windows\System32\lz32.dll
Opens: C:\Windows\System32\apphelp.dll
Opens: C:\Windows\AppPatch\sysmain.sdb
Opens: C:\Windows\Temp\f606c36e9591fbfd0d5f15ddfb01864b.exe
Opens: C:\Windows\AppPatch\AcGenral.dll
Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\SspiCli.dll
Opens: C:\Windows\System32\sspicli.dll
Opens: C:\windows\temp\UxTheme.dll
Opens: C:\Windows\System32\uxtheme.dll
Opens: C:\windows\temp\WINMM.dll
Opens: C:\Windows\System32\winmm.dll
Opens: C:\windows\temp\samcli.dll
Opens: C:\Windows\System32\samcli.dll
Opens: C:\windows\temp\MSACM32.dll
Opens: C:\Windows\System32\msacm32.dll

Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\windows\temp\sfc.dll
Opens: C:\Windows\System32\sfc.dll
Opens: C:\windows\temp\sfc_os.DLL
Opens: C:\Windows\System32\sfc_os.dll
Opens: C:\windows\temp\USERENV.dll
Opens: C:\Windows\System32\userenv.dll
Opens: C:\windows\temp\profapi.dll
Opens: C:\Windows\System32\profapi.dll
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\System32\dwmapi.dll
Opens: C:\windows\temp\MPR.dll
Opens: C:\Windows\System32\mpr.dll
Opens: C:\windows\temp\f606c36e9591fbfd0d5f15ddfb01864b.exe.Manifest
Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\System32\en-US\setupapi.dll.mui
Opens: C:\Windows\Temp
Opens: C:\Windows\Temp\sxeB71E.tmp
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\Temp\sxeB71D.tmp
Opens: C:\
Opens: C:\Windows
Opens: C:\Windows\Temp\sxeB729.tmp
Opens: C:\Windows\Prefetch\SXEB729.TMP-3BAD1DE3.pf
Opens: C:\windows\temp\sxeB729.tmp.Manifest
Opens: C:\Windows\Fonts\sserife.fon
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\System32\rpcss.dll
Opens: C:\windows\temp\CRYPTBASE.dll
Opens: C:\Windows\System32\cryptbase.dll
Writes to: C:\Windows\Temp\sxeB71E.tmp
Writes to: C:\Windows\Temp\sxeB71D.tmp
Writes to: C:\Windows\Temp\sxeB729.tmp
Reads from: C:\Windows\Temp\sxeB71E.tmp
Reads from: C:\Windows\Temp\sxeB729.tmp
Reads from: C:\Windows\Fonts\StaticCache.dat
Deletes: C:\Windows\Temp\sxeB71E.tmp
Deletes: C:\Windows\Temp\sxeB71D.tmp

Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
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\microsoft\windows\currentversion\sidebyside
Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\software\policies\microsoft\windows nt\windows file protection
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\
Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key: HKLM\software\microsoft\oleaut
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\microsoft\windows\currentversion\setup
Opens key: HKLM\software\microsoft\windows\currentversion
Opens key: HKLM\system\currentcontrolset\control\nls\customlocale
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\system\currentcontrolset\services\crypt32
Opens key: HKLM\software\microsoft\windows\currentversion\internet settings
Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet settings
Opens key: HKLM\system\currentcontrolset\control\networkprovider\hworder
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\sxeb729.tmp
Opens key: HKLM\system\currentcontrolset\control\session manager\appcertdlls
Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility
Opens key: HKLM\software\policies\microsoft\windows\appcompat
Opens key: HKCU\software\microsoft\windows\currentversion\explorer\shell folders
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\sxeb729.tmp
Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags
Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
Opens key: HKLM\system\currentcontrolset\control\nls\language groups
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKLM\software\microsoft\ctf\compatibility\sxeb729.tmp
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\ms sans serif
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value: HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[showdebuginfo]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\software\policies\microsoft\windows nt\windows file protection[knowndlllist]

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[f606c36e9591fbfd0d5f15ddfb01864b]
Queries value: HKLM\software\microsoft\windows nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
Queries value: HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
Queries value: HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
Queries value: HKLM\software\microsoft\windows\currentversion[devicepath]
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\services\crypt32[debugheapflags]
Queries value: HKLM\software\microsoft\windows\currentversion\internet settings[disableimprovedzonecheck]
Queries value: HKLM\software\policies\microsoft\windows\currentversion\internet settings[security_hklm_only]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options\dllnxoptions[sxeb71d.tmp]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[authenticodeenabled]
Queries value: HKCU\software\microsoft\windows\currentversion\explorer\shell folders[cache]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\layers[c:\windows\temp\sxeb729.tmp]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags[{ef104bd9-683c-4bf4-a5f5-78fbfcf2c93a}]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[{ef104bd9-683c-4bf4-a5f5-78fbfcf2c93a}]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[{35bf919e-0495-48df-8e74-456384e34e74}]
Queries value: HKLM\software\microsoft\windows nt\currentversion\appcompatflags[{90311299-c714-4367-be12-032f464885b2}]
Queries value: HKCU\software\microsoft\windows nt\currentversion\appcompatflags[{90311299-c714-4367-be12-032f464885b2}]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disablelocaloverride]
Queries value: HKLM\software\microsoft\windows nt\currentversion\compatibility32[sxeb729]
Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409]
Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[disable]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\datastore_v1.0[datafilepath]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane1]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane2]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane3]
Queries value: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback[plane4]
Queries value: HKLM\software\microsoft\windows

nt\currentversion\languagepack\surrogatefallback[plane5]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-
0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\microsoft\ctf[enableanchorcontext]