Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 184, Task ID: 734

Task ID:	734
Risk Level:	1
Date Processed:	2016-04-28 13:07:40 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\25e46fee70fc249c3dafc723a7318696.exe"
Sample ID:	184
Type:	basic
Owner:	admin
Label:	25e46fee70fc249c3dafc723a7318696
Date Added:	2016-04-28 12:45:09 (UTC)
File Type:	PE32:win32:gui
File Size:	583168 bytes
MD5:	25e46fee70fc249c3dafc723a7318696
SHA256:	457e7d6484b6ab34d2d908308284e11c53a22bddf8f23a17e4a69585dc159ec2
Description:	None

Pattern Matching Results

Static Events

Anomaly: PE: Contains a virtual section

Process/Thread Events

Creates process: C:\windows\temp\25e46fee70fc249c3dafc723a7318696.exe
["C:\windows\temp\25e46fee70fc249c3dafc723a7318696.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens: C:\Windows\Prefetch\25E46FEE70FC249C3DAFC723A7318-80C1B302.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\apphelp.dll
Opens: C:\Windows\Temp\25e46fee70fc249c3dafc723a7318696.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\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens: C:\Windows\SysWOW64\winspool.drv
Opens: C:\Windows\SysWOW64\sechost.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\combase.dll

Opens: C:\Windows\SysWOW64\oleaut32.dll
Opens: C:\Windows\SysWOW64\advapi32.dll
Opens: C:\Windows\SysWOW64\gdi32.dll
Opens: C:\Windows\SysWOW64\user32.dll
Opens: C:\Windows\SysWOW64\shlwapi.dll
Opens: C:\Windows\SysWOW64\shell32.dll
Opens: C:\Windows\SysWOW64\ole32.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\SysWOW64\msctf.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.9200.16384_en-us_d51b55b9729b0b41
Opens: C:\Windows\WinSxS\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.9200.16384_en-us_d51b55b9729b0b41\comctl32.dll.mui
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens: C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\riched32.dll
Opens: C:\Windows\SysWOW64\riched20.dll
Opens: C:\Windows\SysWOW64\usp10.dll
Opens: C:\Windows\SysWOW64\msls31.dll
Opens: C:\Windows\win.ini
Opens: C:\Windows\Fonts\tahomabd.ttf
Opens: C:\Windows\Fonts\arial.ttf
Opens: C:\Windows\Fonts\micross.ttf
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Windows\win.ini

Windows Registry Events

Opens key: HKLM\software\microsoft\wow64
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\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\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file
execution options
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions
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\
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\software\wow6432node\microsoft\oleaut
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\software\wow6432node\microsoft\windows nt\currentversion\windows
Opens key: HKCU\software\borland\locales
Opens key: HKLM\software\wow6432node\borland\locales
Opens key: HKCU\software\borland\delphi\locales
Opens key: HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key: HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
Opens key: HKLM\software\policies\microsoft\sqmclient\windows
Opens key: HKLM\software\microsoft\sqmclient\windows
Opens key: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKCU\software\microsoft\windows\currentversion\directmanipulation
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\ids
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\tahoma
Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\25e46fee70fc249c3dafc723a7318696.exe
Opens key: HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
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: 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\image file execution
options\dllnxoptions[usefilter]
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[25e46fee70fc249c3dafc723a7318696.exe]
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[pageallocatorsystemheapisprivate]
Queries value: HKLM\software\microsoft\ole[aggressivemtatesting]
Queries value: HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[25e46fee70fc249c3dafc723a7318696]
Queries value: HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value: HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms
shell dlg 2]
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\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\windows nt\currentversion\fontsubstitutes[tahoma]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinset]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrolldelay]
Queries value: HKCU\software\microsoft\windows nt\currentversion\windows[scrollinterval]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic transparent,0]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic transparent bold,0]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic transparent bold]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[rod transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[helvetica]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[david transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[miriam transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[kaiti_gb2312]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma armenian]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fangsong_gb2312]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tms rmn]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman baltic,186]

Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[helv]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fixed miriam transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms shell dlg]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]