Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 184, Task ID: 737

Task ID:	737
Risk Level:	1
Date Processed:	2016-04-28 13:07:40 (UTC)
Processing Time:	61.17 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
Creates mutex: \Sessions\1\BaseNamedObjects\CicLoadWinStaWinSta0
Creates mutex: \Sessions\1\BaseNamedObjects\MSCTF.CtfMonitorInstMutexDefault1
Creates event: \Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Opens: C:\Windows\Prefetch\25E46FEE70FC249C3DAFC723A7318-80C1B302.pf
Opens: C:\Windows
Opens: C:\Windows\System32\wow64.dll
Opens: C:\Windows\System32\wow64win.dll
Opens: C:\Windows\System32\wow64cpu.dll
Opens: C:\Windows\system32\wow64log.dll
Opens: C:\Windows\SysWOW64
Opens: C:\Windows\SysWOW64\sechost.dll
Opens: C:\windows\temp\version.dll
Opens: C:\Windows\SysWOW64\version.dll
Opens: C:\windows\temp\25e46fee70fc249c3dafc723a7318696.exe.Local\
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll
Opens: C:\windows\temp\winspool.drv
Opens: C:\Windows\SysWOW64\winspool.drv
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\windows\temp\25e46fee70fc249c3dafc723a7318696.ENU
Opens: C:\windows\temp\25e46fee70fc249c3dafc723a7318696.ENU.DLL

Opens: C:\windows\temp\25e46fee70fc249c3dafc723a7318696.EN
Opens: C:\windows\temp\25e46fee70fc249c3dafc723a7318696.EN.DLL
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\SysWOW64\dwmapi.dll
Opens: C:\Windows\Fonts\StaticCache.dat
Opens: C:\Windows\SysWOW64\en-US\user32.dll.mui
Opens: C:\Windows\Globalization\Sorting\SortDefault.nls
Opens: C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.7600.16385_en-us_020378a8991bbcc2
Opens: C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_5.82.7600.16385_en-us_020378a8991bbcc2\comctl32.dll.mui
Opens: C:\Windows\Fonts\tahoma.ttf
Opens: C:\Windows\SysWOW64\uxtheme.dll.Config
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\windows\temp\RICHED32.DLL
Opens: C:\Windows\SysWOW64\riched32.dll
Opens: C:\windows\temp\RICHED20.dll
Opens: C:\Windows\SysWOW64\riched20.dll
Opens: C:\Windows\win.ini
Opens: C:\Windows\SysWOW64\rpcss.dll
Opens: C:\Windows\Fonts\tahomabd.ttf
Opens: C:\Windows\Fonts\arial.ttf
Opens: C:\Windows\SysWOW64\ole32.dll
Reads from: C:\Windows\Fonts\StaticCache.dat
Reads from: C:\Windows\win.ini

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\wow64
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions

Opens key: HKLM\
Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\diagnostics
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: 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: 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\wow6432node\microsoft\windows nt\currentversion\fontsubstitutes
Opens key: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
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\system\currentcontrolset\control\cmf\config
Opens key: HKLM\software\microsoft\windows nt\currentversion\languagepack\surrogatefallback\tahoma
Opens key: HKLM\software\wow6432node\microsoft\ctf\compatibility\25e46fee70fc249c3dafc723a7318696.exe
Opens key: HKCU\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\wow6432node\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
Opens key: HKLM\software\wow6432node\microsoft\ctf\
Opens key: HKLM\software\wow6432node\microsoft\ctf\knownclasses
Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]
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: 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: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
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\software\microsoft\ole[pageallocatorusesystemheap]
Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
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\windows nt\currentversion\fontsubstitutes[ms shell dlg 2]
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\system\currentcontrolset\control\cmf\config[system]
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]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arabic transparent bold]
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[helvetica]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[arial tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[courier new tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman baltic,186]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman ce,238]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman cyr,204]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman greek,161]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[times new roman tur,162]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tahoma armenian]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[helv]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[tms rmn]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[david transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[miriam transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fixed miriam transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[rod transparent]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[fangsong_gb2312]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[kaiti_gb2312]
Queries value: HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes[ms shell dlg]
Queries value: HKLM\software\microsoft\ctf\tip\{0000897b-83df-4b96-be07-0fb58b01c4a4}\languageprofile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}[enable]
Queries value: HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]