Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 35, Task ID: 137

Task ID:	137
Risk Level:	4
Date Processed:	2016-04-28 12:50:33 (UTC)
Processing Time:	60.83 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\42592acde05d7a071f645889ef3ad9f1.exe"

Sample ID:	35
Type:	basic
Owner:	admin
Label:	42592acde05d7a071f645889ef3ad9f1
Date Added:	2016-04-28 12:44:53 (UTC)
File Type:	PE32:win32:gui
File Size:	311152 bytes
MD5:	42592acde05d7a071f645889ef3ad9f1
SHA256:	c15995d5d01cccefa2e55ad26f127b4f5c42bd2601a62ad8ad85d3c2f3156825
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\42592acde05d7a071f645889ef3ad9f1.exe ["C:\windows\temp\42592acde05d7a071f645889ef3ad9f1.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex
Creates mutex:	\Sessions\1\BaseNamedObjects\__KiesTrayAgentRunning__

File System Events

Opens:	C:\Windows\Prefetch\42592ACDE05D7A071F645889EF3AD-1CE383E5.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\42592acde05d7a071f645889ef3ad9f1.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\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\SysWOW64\version.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7
Opens:	C:\Windows\WinSxS\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7\mfc90u.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6871_none_50944e7cbcb706e5
Opens:	C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6871_none_50944e7cbcb706e5\msvcr90.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.6871_none_50944e7cbcb706e5\msvcp90.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\msimg32.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll
Opens:	C:\Windows\SysWOW64\user32.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\cfgmgr32.dll

```
  Opens:                  C:\Windows\SysWOW64\devobj.dll
  Opens:                  C:\Windows\SysWOW64\setupapi.dll
  Opens:                  C:\Windows\SysWOW64\advapi32.dll
  Opens:                  C:\Windows\SysWOW64\shlwapi.dll
  Opens:                  C:\Windows\SysWOW64\shell32.dll
  Opens:                  C:\Windows\SysWOW64\ole32.dll
  Opens:                  C:\Windows\SysWOW64\oleaut32.dll
  Opens:                  C:\Windows\SysWOW64\iertutil.dll
  Opens:                  C:\Windows\SysWOW64\wininet.dll
  Opens:                  C:\Windows\SysWOW64\imm32.dll
  Opens:                  C:\Windows\SysWOW64\msctf.dll
  Opens:                  C:\Windows\WindowsShell.Manifest
  Opens:                  C:\
  Opens:                  C:\Windows\SysWOW64\uxtheme.dll
  Opens:                  C:\Windows\SysWOW64\dwmapi.dll
  Opens:                  C:\Windows\Fonts\arial.ttf
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7\mfc90u.dll.2.Manifest
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7\mfc90u.dll.3.Manifest
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc90.mfc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4bf5400abf9d60b7\mfc90u.dll.Manifest
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc90.mfcloc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4973eb1d754a9dc9
  Opens:
C:\Windows\WinSxS\x86_microsoft.vc90.mfcloc_1fc8b3b9a1e18e3b_9.0.30729.4148_none_4973eb1d754a9dc9\MFC90ENU.DLL
  Opens:                  C:\windows\temp\42592acde05d7a071f645889ef3ad9f1.exe.2.Manifest
  Opens:                  C:\windows\temp\42592acde05d7a071f645889ef3ad9f1.exe.3.Manifest
  Opens:                  C:\windows\temp\42592acde05d7a071f645889ef3ad9f1.exe.Config
  Opens:                  C:\Windows\SysWOW64\UxTheme.dll.Config
  Opens:                  C:\Windows\SysWOW64\msasn1.dll
  Opens:                  C:\Windows\SysWOW64\crypt32.dll
  Opens:                  C:\Windows\SysWOW64\wintrust.dll
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
```

Windows Registry Events

```
  Creates key:            HKCU\software\samsung\kies2.0\setting\setting_general
  Creates key:            HKCU\software
  Creates key:            HKCU\software\samsung
  Creates key:            HKCU\software\samsung\kies2.0
  Creates key:            HKCU\software\samsung\kies2.0\setting
  Opens key:              HKLM\software\microsoft\wow64
  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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  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\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\
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
  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\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:                 HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                 HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:                 HKLM\system\currentcontrolset\control\nls\extendedlocale
  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\policies\microsoft\sqmclient\windows
  Opens key:                 HKLM\software\microsoft\sqmclient\windows
  Opens key:                 HKCU\software\microsoft\windows nt\currentversion\windows
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\network
  Opens key:                 HKCU\software\microsoft\windows\currentversion\policies\comdlg32
  Opens key:                 HKCU\software\microsoft\windows\currentversion\directmanipulation
  Opens key:                 HKCU\software\multistagetrayagent\kies
trayagent\workspace\windowplacement
  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\wow6432node\microsoft\windows
nt\currentversion\fontsubstitutes
  Opens key:                 HKLM\software\microsoft\windows nt\currentversion\fontsubstitutes
  Opens key:                 HKCU\software\microsoft\windows\currentversion\explorer\advanced
  Opens key:                 HKLM\system\setup
  Opens key:                 HKLM\system\currentcontrolset\control\deviceclasses\{3abf6f2d-71c4-462a-
8a92-1e6861e6af27}
  Opens key:                 HKLM\system\currentcontrolset\services\crypt32
  Opens key:                 HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
  Opens key:                 HKLM\system\currentcontrolset\control\nls\sorting\ids
  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[42592acde05d7a071f645889ef3ad9f1.exe]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[42592acde05d7a071f645889ef3ad9f1]
  Queries value:             HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
  Queries value:             HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:             HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  Queries value:             HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
```

```
  Queries value:            HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
  Queries value:            HKLM\software\wow6432node\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\software\microsoft\ole[pageallocatorusesystemheap]
  Queries value:            HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
  Queries value:            HKLM\software\microsoft\ole[aggressivemtatesting]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[dragmindist]
  Queries value:            HKCU\software\microsoft\windows nt\currentversion\windows[dragdelay]
  Queries value:            HKLM\system\currentcontrolset\control\nls\customlocale[en]
  Queries value:            HKLM\system\currentcontrolset\control\nls\extendedlocale[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\fontsubstitutes[segoe
ui]
  Queries value:
HKCU\software\samsung\kies2.0\setting\setting_general[setting_general_isautorunondeviceconnect]
  Queries value:
HKCU\software\samsung\kies2.0\setting\setting_general[setting_general_isautoruncaptureonwinstartup]
  Queries value:            HKCU\control panel\desktop[smoothscroll]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[enableballoontips]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewalphaselect]
  Queries value:
HKCU\software\microsoft\windows\currentversion\explorer\advanced[listviewshadow]
  Queries value:            HKLM\system\setup[systemsetupinprogress]
  Queries value:            HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
  Queries value:            HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
```