

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 35, Task ID: 140

Task ID:	140
Risk Level:	4
Date Processed:	2016-04-28 12:50:36 (UTC)
Processing Time:	62.38 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\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\42592acde05d7a071f645889ef3ad9f1.exe.Local\
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\temp\VERSION.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_9.0.30729.4940_none_50916076bcb9a742
Opens: C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcr90.dll
Opens: C:\windows\temp\MSIMG32.dll
Opens: C:\Windows\SysWOW64\msimg32.dll
Opens: C:\Windows\winsxs\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\msvcpi90.dll
Opens: C:\Windows\SysWOW64\imm32.dll
Opens: C:\Windows\WindowsShell.Manifest
Opens: C:\Windows\SysWOW64\en-US\setupapi.dll.mui
Opens: C:\
Opens: C:\windows\temp\UxTheme.dll
Opens: C:\Windows\SysWOW64\uxtheme.dll
Opens: C:\windows\temp\dwapi.dll
Opens: C:\Windows\SysWOW64\dwapi.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\Temp\42592acde05d7a071f645889ef3ad9f1.exe
Opens:
C:\windows\temp\42592acde05d7a071f645889ef3ad9f1ENU.dll
Opens:
C:\windows\temp\42592acde05d7a071f645889ef3ad9f1LOC.dll
Opens:
C:\Windows\SysWOW64\rpcss.dll
Opens:
C:\Windows\SysWOW64\UxTheme.dll.Config
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\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\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: HKLM\system\currentcontrolset\control\cmf\config
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: HKCU\software\microsoft\windows nt\currentversion\windows
 Opens key: HKLM\system\currentcontrolset\services\crypt32
 Opens key: HKLM\software\wow6432node\microsoft\windows\currentversion\internet
 settings
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows\currentversion\internet settings
 Opens key: HKLM\software\policies\microsoft\windows\currentversion\internet
 settings
 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\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: HKLM\software\wow6432node\microsoft\rpc
 Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername
 Opens key: HKLM\system\setup
 Opens key: HKLM\software\wow6432node\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\windows nt\rpc
 Opens key: HKLM\software\policies\microsoft\sqmclient\windows
 Opens key: HKLM\software\microsoft\sqmclient\windows
 Opens key: HKCU\software\microsoft\windows\currentversion\explorer\advanced
 Opens key: HKLM\software\wow6432node\microsoft\windows nt\currentversion\msasn1
 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\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[alternatetcodepage]
 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[42592acde05d7a071f645889ef3ad9f1]
 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[pageallocatorusesystemheapisprivate]
 Queries value: HKLM\system\currentcontrolset\control\cmf\config[system]
 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: HKCU\software\microsoft\windows nt\currentversion\windows[dragindist]
 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\services\crypt32[debugheapflags]
 Queries value: HKLM\software\wow6432node\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\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: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value: HKLM\system\currentcontrolset\control\computername\activecomputername[computername]

Queries value: HKLM\system\setup[oobeinprogress]

Queries value: HKLM\system\setup\systemsetupinprogress]

Queries value: HKLM\software\microsoft\sqmclient\windows[ceipenable]

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]