Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 147, Task ID: 588

Task ID:	588
Risk Level:	4
Date Processed:	2016-04-28 13:03:06 (UTC)
Processing Time:	61.26 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\09ab0b0cc1afb1e6c115b42828f02a7f.exe"

Sample ID:	147
Type:	basic
Owner:	admin
Label:	09ab0b0cc1afb1e6c115b42828f02a7f
Date Added:	2016-04-28 12:45:05 (UTC)
File Type:	PE32:win32:gui
File Size:	198144 bytes
MD5:	09ab0b0cc1afb1e6c115b42828f02a7f
SHA256:	75cd70342689a10d9c34a1018fc80d4b584892daeea7435d2d7fe94fa2bd560f
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\09ab0b0cc1afb1e6c115b42828f02a7f.exe ["C:\windows\temp\09ab0b0cc1afb1e6c115b42828f02a7f.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:	\KernelObjects\MaximumCommitCondition
Creates event:	\Sessions\1\BaseNamedObjects\MSCTF.CtfActivated.Default1

File System Events

Creates:	C:\Users\Admin\AppData\Local\Temp\7zS6EC7.tmp
Opens:	C:\Windows\Prefetch\09AB0B0CC1AFB1E6C115B42828F02-42473EA8.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\rpcss.dll
Opens:	C:\windows\temp\CRYPTBASE.dll
Opens:	C:\Windows\System32\cryptbase.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\Windows\System32\ExplorerFrame.dll
Opens:	C:\Windows\System32\duser.dll
Opens:	C:\Windows\System32\dui70.dll
Opens:	C:\Windows\Temp\09ab0b0cc1afb1e6c115b42828f02a7f.exe
Opens:	C:\Users\Admin\AppData\Local\Temp
Opens:	C:\Users\Admin\AppData\Local\Temp\7zS6EC7.tmp
Opens:	C:\Windows\Fonts\tahoma.ttf
Opens:	C:\Windows\Temp
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll
Opens:	C:\windows\temp\09ab0b0cc1afb1e6c115b42828f02a7f.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\WindowsShell.Manifest
  Opens:                  C:\Windows\Globalization\Sorting\SortDefault.nls
  Opens:                  C:\Windows\Fonts\StaticCache.dat
  Opens:                  C:\windows\temp\imageres.dll
  Opens:                  C:\Windows\System32\imageres.dll
  Opens:                  C:\Windows\System32\en-US\imageres.dll.mui
  Reads from:             C:\Windows\Temp\09ab0b0cc1afb1e6c115b42828f02a7f.exe
  Reads from:             C:\Windows\Fonts\StaticCache.dat
  Deletes:                C:\Users\Admin\AppData\Local\Temp\7zS6EC7.tmp
```

Windows Registry Events

```
  Creates key:            HKCR\applications\09ab0b0cc1afb1e6c115b42828f02a7f.exe
  Opens key:              HKLM\system\currentcontrolset\control\session manager
  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:              HKLM\system\currentcontrolset\control\nls\sorting\versions
  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\windows nt\currentversion\diagnostics
  Opens key:              HKLM\software\microsoft\ole
  Opens key:              HKLM\software\microsoft\ole\tracing
  Opens key:              HKLM\software\microsoft\oleaut
  Opens key:              HKCU\software\classes\
  Opens key:              HKLM\software\microsoft\com3
  Opens key:              HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}
  Opens key:              HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}
  Opens key:              HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\treatas
  Opens key:              HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\treatas
  Opens key:              HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\progid
  Opens key:              HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\progid
  Opens key:              HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprocserver32
  Opens key:              HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32
  Opens key:              HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprochandler32
  Opens key:              HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprochandler32
  Opens key:              HKCU\software\classes\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprochandler
  Opens key:              HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprochandler
  Opens key:              HKCU\software\classes\applications\09ab0b0cc1afb1e6c115b42828f02a7f.exe
  Opens key:              HKLM\software\classes
  Opens key:              HKLM\software\microsoft\windows\windows error reporting\wmr
  Opens key:              HKLM\system\currentcontrolset\control\nls\customlocale
  Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
  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\currentversion\sidebyside\assemblystorageroots
  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\09ab0b0cc1afb1e6c115b42828f02a7f.exe
  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\ctf\knownclasses
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\software\microsoft\windows\currentversion\policies\explorer
  Opens key:                HKCU\software\microsoft\windows\currentversion\policies\explorer
  Queries value:            HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
  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:            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\microsoft\windows
nt\currentversion\compatibility32[09ab0b0cc1afb1e6c115b42828f02a7f]
  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\software\microsoft\com3[com+enabled]
  Queries value:            HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}[]
  Queries value:            HKCR\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprocserver32[inprocserver32]
  Queries value:            HKCR\clsid\{56fdf344-fd6d-11d0-958a-006097c9a090}\inprocserver32[]
  Queries value:            HKCR\clsid\{56fdf344-fd6d-11d0-958a-
006097c9a090}\inprocserver32[threadingmodel]
  Queries value:            HKLM\software\microsoft\ole[maxsxshashcount]
  Queries value:            HKLM\software\microsoft\windows\windows error reporting\wmr[disable]
  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\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]
  Queries value:              HKLM\system\currentcontrolset\control\cmf\config[system]
  Sets/Creates value:         HKCR\applications\09ab0b0cc1afb1e6c115b42828f02a7f.exe[ishostapp]
```