Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	806
Risk Level:	4
Date Processed:	2016-04-28 13:09:46 (UTC)
Processing Time:	60.59 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9af75510bac6aa983165d40392917512.exe"
Sample ID:	202
Type:	basic
Owner:	admin
Label:	9af75510bac6aa983165d40392917512
Date Added:	2016-04-28 12:45:11 (UTC)
File Type:	PE32:win32:gui
File Size:	443416 bytes
MD5:	9af75510bac6aa983165d40392917512
SHA256:	776b9b4fac717c342ab35fb19f65ac6b4c311ca206fdc844cec2ef84826cc274
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\9af75510bac6aa983165d40392917512.exe
["C:\windows\temp\9af75510bac6aa983165d40392917512.exe"]

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\9AF75510BAC6AA983165D40392917-0F7D552F.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\9af75510bac6aa983165d40392917512.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

Windows Registry Events

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\system\currentcontrolset\control\session manager
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]
```