Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	250
Risk Level:	4
Date Processed:	2016-04-28 12:54:00 (UTC)
Processing Time:	3.26 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\96f3d3abbcd27305649cd81a787d451a.exe"
Sample ID:	63
Type:	basic
Owner:	admin
Label:	96f3d3abbcd27305649cd81a787d451a
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	7680 bytes
MD5:	96f3d3abbcd27305649cd81a787d451a
SHA256:	493811a0d12fe46c5e491c367a17f46da6818ac0eb7f8a47e157e2edfea4c669
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\96f3d3abbcd27305649cd81a787d451a.exe ["C:\windows\temp\96f3d3abbcd27305649cd81a787d451a.exe"]
Terminates process:	C:\Windows\Temp\96f3d3abbcd27305649cd81a787d451a.exe

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\96F3D3ABBCD27305649CD81A787D4-A79467B5.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\96f3d3abbcd27305649cd81a787d451a.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.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:\
Opens:	C:\Windows\SysWOW64\wbem
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0
Opens:	C:\Windows\Temp

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\software\wow6432node\microsoft\windows\currentversion\sidebyside\assemblystorageroots
  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
  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\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[usefilter]
  Queries value:        HKLM\software\microsoft\windows nt\currentversion\image file execution
options\dllnxoptions[96f3d3abbcd27305649cd81a787d451a.exe]
```