Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2459
Risk Level:	5
Date Processed:	2016-02-22 05:32:39 (UTC)
Processing Time:	3.99 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	

`"c:\windows\temp\bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1.exe"`

Sample ID:	628
Type:	basic
Owner:	admin
Label:	bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1
Date Added:	2016-02-22 05:26:50 (UTC)
File Type:	PE32:win32:gui
File Size:	184576 bytes
MD5:	025986b0f09a922b443488294b486a5b
SHA256:	bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1
Description:	None

Pattern Matching Results

`2` PE: Nonstandard section
`5` PE: Contains compressed section

Static Events

Anomaly:	PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:
`C:\windows\temp\bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1.exe`
`["C:\windows\temp\bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1.exe" ]`
Terminates process:
`C:\Windows\Temp\bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1.exe`

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\BAC757C8B1491E9680F23D7EDB787-8995BD37.pf
Opens:	C:\Windows\System32
Opens:	C:\Windows\System32\sechost.dll
Opens:	C:\windows\temp\dbghelp.dll
Opens:	C:\Windows\System32\dbghelp.dll
Opens:	C:\Windows\System32\imm32.dll
Opens:	C:\Windows\System32\uxtheme.dll
Opens:	C:\windows\temp\dwmapi.dll
Opens:	C:\Windows\System32\dwmapi.dll

Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\terminal server
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:              HKLM\system\currentcontrolset\control\nls\customlocale
Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
Opens key:              HKLM\software\microsoft\internet explorer
Queries value:          HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:          HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
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[bac757c8b1491e9680f23d7edb787d0a328edbe68bd7aff645fa23975b13cab1]
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\system\currentcontrolset\control\nls\customlocale[en-us]
Queries value:          HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us]
Queries value:          HKLM\software\microsoft\internet explorer[version]
```