Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2425
Risk Level:	5
Date Processed:	2016-02-22 05:28:39 (UTC)
Processing Time:	61.24 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	

`"c:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe"`

Sample ID:	620
Type:	basic
Owner:	admin
Label:	188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5
Date Added:	2016-02-22 05:26:49 (UTC)
File Type:	PE32:win32:gui
File Size:	838656 bytes
MD5:	0feaaa4adc31728e54b006ab9a7e6afa
SHA256:	188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5
Description:	None

Pattern Matching Results

`5` PE: Contains compressed section

Process/Thread Events

Creates process:
`C:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe`
`["C:\windows\temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe" ]`

Named Object Events

Creates mutex: `\Sessions\1\BaseNamedObjects\DBWinMutex`

File System Events

Opens:	`C:\Windows\Prefetch\188AB310143D0C0C9673D957FCFE7-4BAD8990.pf`
Opens:	`C:\Windows`
Opens:	`C:\Windows\System32\wow64.dll`
Opens:	`C:\Windows\SysWOW64`
Opens:	`C:\Windows\SysWOW64\apphelp.dll`
Opens:	

`C:\Windows\Temp\188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.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\SysWOW64\clusapi.dll`
Opens:	`C:\Windows\SysWOW64\cryptdll.dll`
Opens:	`C:\Windows\SysWOW64\sechost.dll`
Opens:	`C:\Windows\SysWOW64\msvcrt.dll`
Opens:	`C:\Windows\SysWOW64\bcryptprimitives.dll`
Opens:	`C:\Windows\SysWOW64\cryptbase.dll`
Opens:	`C:\Windows\SysWOW64\sspicli.dll`
Opens:	`C:\Windows\SysWOW64\rpcrt4.dll`
Opens:	`C:\Windows\SysWOW64\user32.dll`
Opens:	`C:\Windows\SysWOW64\gdi32.dll`
Opens:	`C:\Windows\SysWOW64\imm32.dll`
Opens:	`C:\Windows\SysWOW64\msctf.dll`
Opens:	`C:\Windows\SysWOW64\cmutil.dll`

```
Opens:                    C:\Windows\SysWOW64\version.dll
Opens:                    C:\Windows\SysWOW64\advapi32.dll
Opens:                    C:\Windows\SysWOW64\dnsapi.dll
Opens:                    C:\Windows\SysWOW64\nsi.dll
Opens:                    C:\Windows\SysWOW64\ws2_32.dll
Opens:                    C:\Windows\SysWOW64\IPHLPAPI.DLL
Opens:                    C:\Windows\SysWOW64\winnsi.dll
Opens:                    C:\Windows\SysWOW64\mswsock.dll
Opens:                    C:\Windows\SysWOW64\combase.dll
Opens:                    C:\Windows\SysWOW64\ole32.dll
Opens:                    C:\Windows\SysWOW64\oleaut32.dll
Opens:                    C:\Windows\SysWOW64\psapi.dll
Opens:                    C:\Windows\SysWOW64\shlwapi.dll
Opens:                    C:\Windows\SysWOW64\shell32.dll
Opens:                    C:\Windows\SysWOW64\iertutil.dll
Opens:                    C:\Windows\SysWOW64\wininet.dll
```

Windows Registry Events

```
Opens key:            HKLM\software\microsoft\wow64
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\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
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
Opens key:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy
Opens key:            HKLM\system\currentcontrolset\control\lsa
Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
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\
Opens key:            HKLM\software\wow6432node\microsoft\windows nt\currentversion\windows
```

```
Opens key:                    HKLM\system\currentcontrolset\control\nls\extendedlocale
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
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:                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]
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[188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5.exe]
Queries value:                HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
Queries value:                HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
Queries value:                HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
Queries value:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[188ab310143d0c0c9673d957fcfe757877037611aa31c9d11179890201e276c5]
Queries value:                HKLM\software\wow6432node\microsoft\windows
nt\currentversion\windows[loadappinit_dlls]
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\ole[pageallocatorusesystemheap]
Queries value:                HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate]
Queries value:                HKLM\software\microsoft\ole[aggressivemtatesting]
```