Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	2401
Risk Level:	5
Date Processed:	2016-02-22 05:26:51 (UTC)
Processing Time:	61.26 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe"

Sample ID:	614
Type:	basic
Owner:	admin
Label:	7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20
Date Added:	2016-02-22 05:26:48 (UTC)
File Type:	PE32:win32:gui
File Size:	55808 bytes
MD5:	093586512549f2d016ad4c70f4f8e5c8
SHA256:	7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20
Description:	None

Pattern Matching Results

5 PE: Contains compressed section

Process/Thread Events

Creates process:
C:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe ["C:\windows\temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\7A495357099319383D3E509A676B5-49B7ACAE.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.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\regapi.dll
Opens:	C:\Windows\SysWOW64\sqlunirl.dll
Opens:	C:\Windows\SysWOW64\winspool.drv
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.9200.16384_none_bf100cd445f4d954\comctl32.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\combase.dll
Opens:	C:\Windows\SysWOW64\SHCore.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\advapi32.dll
  Opens:                  C:\Windows\SysWOW64\psapi.dll
  Opens:                  C:\Windows\SysWOW64\gdi32.dll
  Opens:                  C:\Windows\SysWOW64\user32.dll
  Opens:                  C:\Windows\SysWOW64\shlwapi.dll
  Opens:                  C:\Windows\SysWOW64\shell32.dll
  Opens:                  C:\Windows\SysWOW64\comdlg32.dll
  Opens:                  C:\Windows\SysWOW64\imm32.dll
  Opens:                  C:\Windows\SysWOW64\msctf.dll
  Opens:                  C:\Windows\SysWOW64\nddeapi.dll
  Opens:                  C:\Windows\SysWOW64\cmdial32.dll
  Opens:                  C:\Windows\SysWOW64\cmpbk32.dll
  Opens:                  C:\Windows\SysWOW64\cmutil.dll
  Opens:                  C:\Windows\SysWOW64\eappcfg.dll
  Opens:                  C:\Windows\SysWOW64\userenv.dll
  Opens:                  C:\Windows\SysWOW64\profapi.dll
  Opens:                  C:\Windows\SysWOW64\ole32.dll
  Opens:                  C:\Windows\SysWOW64\cfgmgr32.dll
  Opens:                  C:\Windows\SysWOW64\devobj.dll
  Opens:                  C:\Windows\SysWOW64\setupapi.dll
  Opens:                  C:\Windows\SysWOW64\oleaut32.dll
  Opens:                  C:\Windows\SysWOW64\en-US\setupapi.dll.mui
```

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\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
  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\software\wow6432node\microsoft\ole
  Opens key:                HKLM\software\microsoft\ole
  Opens key:                HKLM\software\wow6432node\microsoft\ole\tracing
  Opens key:                HKLM\software\microsoft\ole\tracing
  Opens key:                HKLM\software\policies\microsoft\sqmclient\windows
  Opens key:                HKLM\software\microsoft\sqmclient\windows
  Opens key:                HKCU\software\microsoft\microsoft sql server\80\tools\client
  Opens key:                HKCU\software\microsoft\microsoft sql server\80\tools\sqlstr
  Opens key:                HKLM\system\currentcontrolset\control\cmf\config
  Opens key:                HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\microsoft\windows\currentversion\setup
  Opens key:                HKLM\software\wow6432node\microsoft\windows\currentversion
  Opens key:                HKLM\system\currentcontrolset\control\nls\extendedlocale
  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[7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20.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[7a495357099319383d3e509a676b5bd5876f0d9f4dd8a16bea1dd3424ed95c20]
  Queries value:            HKLM\software\wow6432node\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\ole[aggressivemtatesting]
  Queries value:            HKLM\software\microsoft\sqmclient\windows[ceipenable]
  Queries value:            HKLM\system\currentcontrolset\control\cmf\config[system]
  Queries value:            HKLM\software\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
```

```
   Queries value:              HKLM\software\microsoft\windows\currentversion\setup[sourcepath]
   Queries value:              HKLM\software\wow6432node\microsoft\windows\currentversion[devicepath]
   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\wmi\security[5f31090b-d990-4e91-
b16d-46121d0255aa]
```