Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	702
Risk Level:	5
Date Processed:	2016-04-28 13:06:31 (UTC)
Processing Time:	61.07 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\5a9a5eeee9b778e5b0ddbda6444592c5.exe"
Sample ID:	176
Type:	basic
Owner:	admin
Label:	5a9a5eeee9b778e5b0ddbda6444592c5
Date Added:	2016-04-28 12:45:08 (UTC)
File Type:	PE32:win32:gui
File Size:	704296 bytes
MD5:	5a9a5eeee9b778e5b0ddbda6444592c5
SHA256:	2476122146c71214ce1a59c9f47bcab169e4ce30b04e305a7cda4dfec8053f92
Description:	None

Pattern Matching Results

`5` Resource section contains an executable
`2` 64 bit executable
`5` Possible injector

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Resource section contains an executable

Process/Thread Events

Creates process:	C:\windows\temp\5a9a5eeee9b778e5b0ddbda6444592c5.exe

["C:\windows\temp\5a9a5eeee9b778e5b0ddbda6444592c5.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\5A9A5EEEE9B778E5B0DDBDA644459-8DD2E727.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\5a9a5eeee9b778e5b0ddbda6444592c5.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\mpr.dll
Opens:	C:\Windows\SysWOW64\version.dll
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985
Opens:	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.9200.16384_none_893961408605e985\comctl32.dll
Opens:	C:\Windows\SysWOW64\sechost.dll
Opens:	C:\Windows\SysWOW64\SHCore.dll
Opens:	C:\Windows\SysWOW64\gdi32.dll

```
Opens:              C:\Windows\SysWOW64\user32.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\combase.dll
Opens:              C:\Windows\SysWOW64\oleaut32.dll
Opens:              C:\Windows\SysWOW64\advapi32.dll
Opens:              C:\Windows\SysWOW64\ole32.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\WindowsShell.Manifest
Opens:              C:\Windows\SysWOW64\uxtheme.dll
Opens:              C:\Windows\SysWOW64\dwmapi.dll
Opens:              C:\Windows\Globalization\Sorting\SortDefault.nls
Opens:              C:\Windows\SysWOW64\netmsg.dll
Opens:              C:\Windows\Fonts\StaticCache.dat
Opens:              C:\Windows\SysWOW64\imageres.dll
Reads from:         C:\Windows\Temp\5a9a5eeee9b778e5b0ddbda6444592c5.exe
Reads from:         C:\Windows\Fonts\StaticCache.dat
```

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
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
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\lsa\fipsalgorithmpolicy
   Opens key:              HKLM\system\currentcontrolset\control\lsa
   Opens key:
HKLM\system\currentcontrolset\policies\microsoft\cryptography\configuration
   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
   Opens key:              HKLM\system\currentcontrolset\control\networkprovider\hworder
   Opens key:              HKLM\software\wow6432node\microsoft\windows\windows error reporting\wmr
   Opens key:              HKLM\system\currentcontrolset\control\nls\extendedlocale
   Opens key:              HKLM\software\policies\microsoft\sqmclient\windows
   Opens key:              HKLM\software\microsoft\sqmclient\windows
   Opens key:              HKCU\software\microsoft\windows\currentversion\directmanipulation
   Opens key:
HKLM\software\wow6432node\microsoft\ctf\compatibility\5a9a5eeee9b778e5b0ddbda6444592c5.exe
   Opens key:              HKLM\software\wow6432node\microsoft\ctf\
   Opens key:              HKLM\system\currentcontrolset\control\nls\sorting\ids
   Opens key:              HKLM\software\wow6432node\microsoft\ctf\knownclasses
   Opens key:              HKLM\system\currentcontrolset\control\nls\locale
   Opens key:              HKLM\system\currentcontrolset\control\nls\locale\alternate sorts
   Opens key:              HKLM\system\currentcontrolset\control\nls\language groups
   Opens key:              HKLM\software\microsoft\windows nt\currentversion\fontlink\systemlink
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback
   Opens key:              HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback\segoe ui
   Opens key:
HKLM\software\wow6432node\microsoft\windows\currentversion\policies\explorer
   Opens key:              HKLM\software\microsoft\windows\currentversion\policies\explorer
   Opens key:              HKCU\software\microsoft\windows\currentversion\policies\explorer
   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[5a9a5eeee9b778e5b0ddbda6444592c5.exe]
   Queries value:          HKLM\software\microsoft\windows
nt\currentversion\gre_initialize[disablemetafiles]
   Queries value:          HKLM\software\wow6432node\microsoft\windows
nt\currentversion\compatibility32[5a9a5eeee9b778e5b0ddbda6444592c5]
   Queries value:          HKLM\software\wow6432node\microsoft\windows
```

```
nt\currentversion\windows[loadappinit_dlls]
  Queries value:             HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:             HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
  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\wow6432node\microsoft\windows\windows error
reporting\wmr[disable]
  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\sqmclient\windows[ceipenable]
  Queries value:             HKLM\software\wow6432node\microsoft\ctf[enableanchorcontext]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\versions[000602xx]
  Queries value:             HKLM\system\currentcontrolset\control\nls\locale[00000409]
  Queries value:             HKLM\system\currentcontrolset\control\nls\language groups[1]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[disable]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\datastore_v1.0[datafilepath]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane1]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane2]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane3]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane4]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane5]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane6]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane7]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane8]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane9]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane10]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane11]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane12]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane13]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane14]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane15]
  Queries value:             HKLM\software\microsoft\windows
nt\currentversion\languagepack\surrogatefallback[plane16]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\ids[en-us]
  Queries value:             HKLM\system\currentcontrolset\control\nls\sorting\ids[en]
  Queries value:
HKLM\software\microsoft\windows\currentversion\policies\explorer[turnoffspianimations]
```