Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	791
Risk Level:	5
Date Processed:	2016-05-18 10:38:44 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe"

Sample ID:	3321
Type:	basic
Owner:	admin
Label:	543bd82ec71ae746e83c14eba28494df
Date Added:	2016-05-18 10:30:50 (UTC)
File Type:	PE32:win32:gui
File Size:	147968 bytes
MD5:	543bd82ec71ae746e83c14eba28494df
SHA256:	b5835739dfcf21ab4869dea949ccc6038ea65be94f11307154e2c58a404b53ec
Description:	None

Pattern Matching Results

5	PE: Contains compressed section
4	Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe ["C:\windows\temp\543bd82ec71ae746e83c14eba28494df.exe"]

Named Object Events

Creates mutex:	\Sessions\1\BaseNamedObjects\DBWinMutex

File System Events

Opens:	C:\Windows\Prefetch\543BD82EC71AE746E83C14EBA2849-6D9DAEDC.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\Windows\SysWOW64\apphelp.dll
Opens:	C:\Windows\Temp\543bd82ec71ae746e83c14eba28494df.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\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\iertutil.dll
Opens:	C:\Windows\SysWOW64\wininet.dll
Opens:	C:\Windows\SysWOW64\advapi32.dll
Opens:	C:\Windows\SysWOW64\mylib\myfile

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 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
  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[543bd82ec71ae746e83c14eba28494df.exe]
  Queries value:            HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]
  Queries value:            HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]
```