Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Task ID:	112
Risk Level:	4
Date Processed:	2016-04-28 12:49:54 (UTC)
Processing Time:	62.34 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\bd6af74bd07ec33b620a90ab69678bc1.exe"

Sample ID:	28
Type:	basic
Owner:	admin
Label:	bd6af74bd07ec33b620a90ab69678bc1
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	245248 bytes
MD5:	bd6af74bd07ec33b620a90ab69678bc1
SHA256:	1a4bc899d17ec74f12250f999f53511d74db6ac00f4660f48cb19b2d7d13cb21
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\bd6af74bd07ec33b620a90ab69678bc1.exe ["C:\windows\temp\bd6af74bd07ec33b620a90ab69678bc1.exe"]

File System Events

Opens:	C:\Windows\Prefetch\BD6AF74BD07EC33B620A90AB69678-1E9F24AE.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\windows\temp\sqlite3.dll
Opens:	C:\Windows\SysWOW64\sqlite3.dll
Opens:	C:\Windows\system\sqlite3.dll
Opens:	C:\Windows\sqlite3.dll
Opens:	C:\Windows\SysWOW64\Wbem\sqlite3.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\sqlite3.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
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
Queries value:	HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]

```
   Queries value:                HKLM\system\currentcontrolset\control\session
manager[cwdillegalindllsearch]
   Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
```