Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 130, Task ID: 521

Task ID:	521
Risk Level:	4
Date Processed:	2016-04-28 13:01:23 (UTC)
Processing Time:	61.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ada3f051bedc650553af52d9321bec2c.exe"
Sample ID:	130
Type:	basic
Owner:	admin
Label:	ada3f051bedc650553af52d9321bec2c
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	245248 bytes
MD5:	ada3f051bedc650553af52d9321bec2c
SHA256:	ec0425791646e77dcaa471392c2d53da3c0ba4fd1523c305d38189cd42c692be
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\windows\temp\ada3f051bedc650553af52d9321bec2c.exe ["C:\windows\temp\ada3f051bedc650553af52d9321bec2c.exe"]

File System Events

Opens:	C:\Windows\Prefetch\ADA3F051BEDC650553AF52D9321BE-3735874B.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]