Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 50, Task ID: 200

Task ID:	200
Risk Level:	4
Date Processed:	2016-04-28 12:52:27 (UTC)
Processing Time:	61.11 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\27c399c97ce41ca4b8add08cfeeb59b2.exe"
Sample ID:	50
Type:	basic
Owner:	admin
Label:	27c399c97ce41ca4b8add08cfeeb59b2
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	91960 bytes
MD5:	27c399c97ce41ca4b8add08cfeeb59b2
SHA256:	a8306a2fa5ac6b6f7e50a3f073525d03c38ceeac53fe0f9884c2682e11e7bd9f
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\27c399c97ce41ca4b8add08cfeeb59b2.exe ["C:\windows\temp\27c399c97ce41ca4b8add08cfeeb59b2.exe"]

File System Events

Opens: C:\Windows\Prefetch\27C399C97CE41CA4B8ADD08CFEEB5-86E7C903.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\RegisterLib.dll
Opens: C:\Windows\SysWOW64\RegisterLib.dll
Opens: C:\Windows\system\RegisterLib.dll
Opens: C:\Windows\RegisterLib.dll
Opens: C:\Windows\SysWOW64\Wbem\RegisterLib.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\RegisterLib.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]