Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 90, Task ID: 361

Task ID:	361
Risk Level:	4
Date Processed:	2016-04-28 12:57:13 (UTC)
Processing Time:	2.32 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\908a5593244da2338e439c239e6e92ab.exe"
Sample ID:	90
Type:	basic
Owner:	admin
Label:	908a5593244da2338e439c239e6e92ab
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	69216 bytes
MD5:	908a5593244da2338e439c239e6e92ab
SHA256:	1cca6e5137a1d81f3c38af1571e02085021814857e8b805d34e1f8a46e118cb5
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\908a5593244da2338e439c239e6e92ab.exe ["C:\windows\temp\908a5593244da2338e439c239e6e92ab.exe"]
Terminates process: C:\Windows\Temp\908a5593244da2338e439c239e6e92ab.exe

File System Events

Opens: C:\Windows\Prefetch\908A5593244DA2338E439C239E6E9-CDE91EAB.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\DriverReviverSetup.exe
Opens: C:\windows\temp\DriverReviverSetup.exe.exe

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
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]