Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 46, Task ID: 184

Task ID:	184
Risk Level:	4
Date Processed:	2016-04-28 12:52:13 (UTC)
Processing Time:	61.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\9da1f1c6f368f12ea0c2bfbdeb766882.exe"
Sample ID:	46
Type:	basic
Owner:	admin
Label:	9da1f1c6f368f12ea0c2bfbdeb766882
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	505344 bytes
MD5:	9da1f1c6f368f12ea0c2bfbdeb766882
SHA256:	f79b8bae0dbd7eb2d3a17c966ab187b0ae91ae5df7d4e41759796a2240bb3f8d
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\windows\temp\9da1f1c6f368f12ea0c2bfbdeb766882.exe
["C:\windows\temp\9da1f1c6f368f12ea0c2bfbdeb766882.exe"]

File System Events

Opens: C:\Windows\Prefetch\9DA1F1C6F368F12EA0C2BFBDEB766-AA5437C8.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\BASS.dll
Opens: C:\Windows\SysWOW64\BASS.dll
Opens: C:\Windows\system\BASS.dll
Opens: C:\Windows\BASS.dll
Opens: C:\Windows\SysWOW64\Wbem\BASS.dll
Opens: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\BASS.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]