Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 80, Task ID: 319

Task ID:	319
Risk Level:	4
Date Processed:	2016-04-28 12:56:01 (UTC)
Processing Time:	61.14 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\8fd748a6f18e76796d0e274593740b83.exe"
Sample ID:	80
Type:	basic
Owner:	admin
Label:	8fd748a6f18e76796d0e274593740b83
Date Added:	2016-04-28 12:44:58 (UTC)
File Type:	PE32:win32:gui
File Size:	668160 bytes
MD5:	8fd748a6f18e76796d0e274593740b83
SHA256:	9dc17f9f85a9bc308a385c41400b31e6f7a60ad9bafdaa64c994a652bf2f0046
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\8fd748a6f18e76796d0e274593740b83.exe ["c:\windows\temp\8fd748a6f18e76796d0e274593740b83.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\8FD748A6F18E76796D0E274593740-0652AE93.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\wsock32.dll
Opens: C:\WINDOWS\system32\ws2_32.dll
Opens: C:\WINDOWS\system32\ws2help.dll
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens: C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens: C:\WINDOWS\system32\winmm.dll

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\8fd748a6f18e76796d0e274593740b83.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]