Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 57, Task ID: 227

Task ID:	227
Risk Level:	1
Date Processed:	2016-04-28 12:53:41 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\600497742f11729df78f50577e2e6dfc.exe"
Sample ID:	57
Type:	basic
Owner:	admin
Label:	600497742f11729df78f50577e2e6dfc
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	372736 bytes
MD5:	600497742f11729df78f50577e2e6dfc
SHA256:	7c867fae813d162fa6dc3d43c8ee89f62ba7cf949b7b17887e1c2ae83a028061
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\600497742f11729df78f50577e2e6dfc.exe ["c:\windows\temp\600497742f11729df78f50577e2e6dfc.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\600497742F11729DF78F50577E2E6-05066B23.pf
Opens: C:\Documents and Settings\Admin
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

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\600497742f11729df78f50577e2e6dfc.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
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
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]