Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 51, Task ID: 203

Task ID:	203
Risk Level:	4
Date Processed:	2016-04-28 12:52:30 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6042f2e158929323e1f7ef4aeadd6d82.exe"
Sample ID:	51
Type:	basic
Owner:	admin
Label:	6042f2e158929323e1f7ef4aeadd6d82
Date Added:	2016-04-28 12:44:55 (UTC)
File Type:	PE32:win32:gui
File Size:	260568 bytes
MD5:	6042f2e158929323e1f7ef4aeadd6d82
SHA256:	5de9c26d1c7ec9a51801ec4db737a73c96fd44235d35f5f2e82bb35d3917f143
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\6042f2e158929323e1f7ef4aeadd6d82.exe ["c:\windows\temp\6042f2e158929323e1f7ef4aeadd6d82.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\6042F2E158929323E1F7EF4AEADD6-0EF27500.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\6042f2e158929323e1f7ef4aeadd6d82.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]