Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 1, Task ID: 2

Task ID:	2
Risk Level:	1
Date Processed:	2016-04-28 12:46:38 (UTC)
Processing Time:	63.68 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\21354e5538706ad6b28941f656b70119.exe"
Sample ID:	1
Type:	basic
Owner:	admin
Label:	21354e5538706ad6b28941f656b70119
Date Added:	2016-04-28 12:44:49 (UTC)
File Type:	PE32:win32:gui
File Size:	65536 bytes
MD5:	21354e5538706ad6b28941f656b70119
SHA256:	38cfeb218e204b232bddc8a071f201d0932bfce0fae32fa344e750cbd2278c9f
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\21354e5538706ad6b28941f656b70119.exe ["c:\windows\temp\21354e5538706ad6b28941f656b70119.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\21354E5538706AD6B28941F656B70-02AFDC08.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\21354e5538706ad6b28941f656b70119.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]