Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 17, Task ID: 66

Task ID:	66
Risk Level:	1
Date Processed:	2016-04-28 12:48:26 (UTC)
Processing Time:	61.23 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\7a40d76e9fa341618d44f168752f6c0f.exe"

Sample ID:	17
Type:	basic
Owner:	admin
Label:	7a40d76e9fa341618d44f168752f6c0f
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	61440 bytes
MD5:	7a40d76e9fa341618d44f168752f6c0f
SHA256:	4d27b0fd517894fd083418585b34b5497c14dfdbf006241a525d954700804a92
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\7a40d76e9fa341618d44f168752f6c0f.exe ["c:\windows\temp\7a40d76e9fa341618d44f168752f6c0f.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\7A40D76E9FA341618D44F168752F6-2DF5FE8B.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\7a40d76e9fa341618d44f168752f6c0f.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]