Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 24, Task ID: 94

Task ID:	94
Risk Level:	1
Date Processed:	2016-04-28 12:49:02 (UTC)
Processing Time:	2.21 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\3d9a2ec042f97b86cf02fa354ba1414d.exe"
Sample ID:	24
Type:	basic
Owner:	admin
Label:	3d9a2ec042f97b86cf02fa354ba1414d
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	45056 bytes
MD5:	3d9a2ec042f97b86cf02fa354ba1414d
SHA256:	c4e23a6b058dea1117941098c2090cab10503baa730f895eae2e10a259e3c5c6
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\WINDOWS\Temp\3d9a2ec042f97b86cf02fa354ba1414d.exe ["c:\windows\temp\3d9a2ec042f97b86cf02fa354ba1414d.exe"]
Terminates process: C:\WINDOWS\Temp\3d9a2ec042f97b86cf02fa354ba1414d.exe

File System Events

Opens: C:\WINDOWS\Prefetch\3D9A2EC042F97B86CF02FA354BA14-011853FE.pf
Opens: C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\3d9a2ec042f97b86cf02fa354ba1414d.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]