Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 44, Task ID: 174

Task ID:	174
Risk Level:	5
Date Processed:	2016-04-28 12:51:55 (UTC)
Processing Time:	62.16 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\fed7d538ffa814cbc2f2a54af94216d3.exe"
Sample ID:	44
Type:	basic
Owner:	admin
Label:	fed7d538ffa814cbc2f2a54af94216d3
Date Added:	2016-04-28 12:44:54 (UTC)
File Type:	PE32:win32:gui
File Size:	444416 bytes
MD5:	fed7d538ffa814cbc2f2a54af94216d3
SHA256:	3143b6299c209ff8ac9144cf2205b0eb247ba7e704da0acfa11887d16fbcee85
Description:	None

Pattern Matching Results

5 Packer: Asprotect
2 PE: Nonstandard section
5 PE: Contains compressed section

Static Events

Anomaly:	PE: Contains a virtual section
Anomaly:	PE: Contains one or more non-standard sections
Packer:	ASProtect

Process/Thread Events

Creates process: C:\WINDOWS\Temp\fed7d538ffa814cbc2f2a54af94216d3.exe ["c:\windows\temp\fed7d538ffa814cbc2f2a54af94216d3.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\FED7D538FFA814CBC2F2A54AF9421-2589A2CD.pf
Opens:	C:\Documents and Settings\Admin

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\fed7d538ffa814cbc2f2a54af94216d3.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]