Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 90, Task ID: 359

Task ID:	359
Risk Level:	4
Date Processed:	2016-04-28 12:56:59 (UTC)
Processing Time:	2.23 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\908a5593244da2338e439c239e6e92ab.exe"
Sample ID:	90
Type:	basic
Owner:	admin
Label:	908a5593244da2338e439c239e6e92ab
Date Added:	2016-04-28 12:44:59 (UTC)
File Type:	PE32:win32:gui
File Size:	69216 bytes
MD5:	908a5593244da2338e439c239e6e92ab
SHA256:	1cca6e5137a1d81f3c38af1571e02085021814857e8b805d34e1f8a46e118cb5
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\908a5593244da2338e439c239e6e92ab.exe ["c:\windows\temp\908a5593244da2338e439c239e6e92ab.exe"]
Terminates process: C:\WINDOWS\Temp\908a5593244da2338e439c239e6e92ab.exe

File System Events

Opens: C:\WINDOWS\Prefetch\908A5593244DA2338E439C239E6E9-217C491B.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\windows\temp\DriverReviverSetup.exe

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\908a5593244da2338e439c239e6e92ab.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Opens key: HKLM\system\currentcontrolset\control\session manager
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\session manager[safeprocesssearchmode]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]