

Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 90, Task ID: 360

Task ID:	360
Risk Level:	4
Date Processed:	2016-04-28 12:57:13 (UTC)
Processing Time:	2.43 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-CDE91EAB.pf
Opens:	C:\Windows\System32
Opens:	C:\windows\temp\DriverReviverSetup.exe
Opens:	C:\windows\temp\DriverReviverSetup.exe.exe

Windows Registry Events

Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\system\currentcontrolset\control\srp\gp\dll
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\system\currentcontrolset\control\nls\sorting\versions
Queries value:	HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value:	HKLM\system\currentcontrolset\control\nls\sorting\versions[]
Queries value:	HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]