Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 23, Task ID: 90

Task ID:	90
Risk Level:	4
Date Processed:	2016-04-28 12:48:53 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\3d3153fe8f8692117697828274214ee6.exe"

Sample ID:	23
Type:	basic
Owner:	admin
Label:	3d3153fe8f8692117697828274214ee6
Date Added:	2016-04-28 12:44:52 (UTC)
File Type:	PE32:win32:gui
File Size:	315392 bytes
MD5:	3d3153fe8f8692117697828274214ee6
SHA256:	06645c8156462a318598c1ec5ea070cfebde6031b9f696925e62f39ac36a91a6
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\3d3153fe8f8692117697828274214ee6.exe ["c:\windows\temp\3d3153fe8f8692117697828274214ee6.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\3D3153FE8F8692117697828274214-37CC9432.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
Opens:	C:\WINDOWS\system32\winspool.drv
Opens:	C:\WINDOWS\system32\oledlg.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\3d3153fe8f8692117697828274214ee6.exe
Opens key:	HKLM\system\currentcontrolset\control\terminal server
Opens key:	HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key:	HKLM\system\currentcontrolset\control\safeboot\option
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value:	HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]