Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 128, Task ID: 511

Task ID:	511
Risk Level:	4
Date Processed:	2016-04-28 13:01:20 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\ad42299d3c0f8ef95821ec8e60db3d30.exe"
Sample ID:	128
Type:	basic
Owner:	admin
Label:	ad42299d3c0f8ef95821ec8e60db3d30
Date Added:	2016-04-28 12:45:03 (UTC)
File Type:	PE32:win32:gui
File Size:	36640 bytes
MD5:	ad42299d3c0f8ef95821ec8e60db3d30
SHA256:	b2be4c83533fc9c68f3a0bcd6805763e1c375183a1b207f7da16710ff60c4c74
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process:	C:\WINDOWS\Temp\ad42299d3c0f8ef95821ec8e60db3d30.exe ["c:\windows\temp\ad42299d3c0f8ef95821ec8e60db3d30.exe"]

File System Events

Opens:	C:\WINDOWS\Prefetch\AD42299D3C0F8EF95821EC8E60DB3-11188812.pf
Opens:	C:\Documents and Settings\Admin
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.MFC_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_a57c1f53\mfc90u.dll
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e
Opens:	C:\WINDOWS\WinSxS\x86_Microsoft.VC90.CRT_1fc8b3b9a1e18e3b_9.0.30729.4148_x-ww_d495ac4e\msvcr90.dll
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\msimg32.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options\ad42299d3c0f8ef95821ec8e60db3d30.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]