Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 63, Task ID: 251

Task ID:	251
Risk Level:	4
Date Processed:	2016-04-28 12:54:00 (UTC)
Processing Time:	2.31 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\96f3d3abbcd27305649cd81a787d451a.exe"
Sample ID:	63
Type:	basic
Owner:	admin
Label:	96f3d3abbcd27305649cd81a787d451a
Date Added:	2016-04-28 12:44:56 (UTC)
File Type:	PE32:win32:gui
File Size:	7680 bytes
MD5:	96f3d3abbcd27305649cd81a787d451a
SHA256:	493811a0d12fe46c5e491c367a17f46da6818ac0eb7f8a47e157e2edfea4c669
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\96f3d3abbcd27305649cd81a787d451a.exe ["c:\windows\temp\96f3d3abbcd27305649cd81a787d451a.exe"]
Terminates process: C:\WINDOWS\Temp\96f3d3abbcd27305649cd81a787d451a.exe

File System Events

Opens: C:\WINDOWS\Prefetch\96F3D3ABBCD27305649CD81A787D4-1911F96C.pf
Opens: C:\Documents and Settings\Admin
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:\
Opens: C:\WINDOWS
Opens: C:\WINDOWS\system32
Opens: C:\WINDOWS\system32\wbem
Opens: C:\WINDOWS\Temp

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\96f3d3abbcd27305649cd81a787d451a.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
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\msvcr90.dll
Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\ntdll.dll
Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options\kernel32.dll
Opens key: HKCU\
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value:
HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]
Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]
Queries value: HKCU\control panel\desktop[multiuilanguageid]