Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 164, Task ID: 655

Task ID:	655
Risk Level:	4
Date Processed:	2016-04-28 13:04:50 (UTC)
Processing Time:	61.08 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\6236837781d95097a3d344416cee37ba.exe"
Sample ID:	164
Type:	basic
Owner:	admin
Label:	6236837781d95097a3d344416cee37ba
Date Added:	2016-04-28 12:45:07 (UTC)
File Type:	PE32:win32:gui
File Size:	582104 bytes
MD5:	6236837781d95097a3d344416cee37ba
SHA256:	1432270e6b4e1ebdf7ff1221833791340a87beaaaad578f3e9f1f09c05fb412b
Description:	None

Pattern Matching Results

4 Checks whether debugger is present

Process/Thread Events

Creates process: C:\WINDOWS\Temp\6236837781d95097a3d344416cee37ba.exe ["c:\windows\temp\6236837781d95097a3d344416cee37ba.exe"]

File System Events

Opens: C:\WINDOWS\Prefetch\6236837781D95097A3D344416CEE3-3568684C.pf
Opens: C:\Documents and Settings\Admin
Opens: C:\WINDOWS\system32\winmm.dll

Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\6236837781d95097a3d344416cee37ba.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
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]