Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 7, Task ID: 27

Task ID:	27
Risk Level:	1
Date Processed:	2016-04-28 12:46:44 (UTC)
Processing Time:	62.48 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\83aeb82d5c10754e84f518377a34999a.exe"
Sample ID:	7
Type:	basic
Owner:	admin
Label:	83aeb82d5c10754e84f518377a34999a
Date Added:	2016-04-28 12:44:50 (UTC)
File Type:	PE32:win32:gui
File Size:	253952 bytes
MD5:	83aeb82d5c10754e84f518377a34999a
SHA256:	04ea191c4d621fd07c1c42cfdcf94d58685ff5458197b59d09cf72e1f097c058
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\83aeb82d5c10754e84f518377a34999a.exe ["C:\windows\temp\83aeb82d5c10754e84f518377a34999a.exe"]

File System Events

Opens: C:\Windows\Prefetch\83AEB82D5C10754E84F518377A349-3BCC4780.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\alleg40.dll
Opens: C:\Windows\system32\alleg40.dll
Opens: C:\Windows\system\alleg40.dll
Opens: C:\Windows\alleg40.dll
Opens: C:\Windows\System32\Wbem\alleg40.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\alleg40.dll

Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\terminal server
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: HKCU\
Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration
Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration
Opens key: HKCU\control panel\desktop
Opens key: HKCU\control panel\desktop\muicached
Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsuserenabled]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

Queries value: HKCU\control panel\desktop[preferreduilanguages]
Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]
Queries value:
HKLM\software\microsoft\windows\currentversion\sidebyside[preferexternalmanifest]