Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 113, Task ID: 453

Task ID:	453
Risk Level:	1
Date Processed:	2016-04-28 12:59:27 (UTC)
Processing Time:	61.1 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\71cfa0de4981df28171710cf03332a99.exe"

Sample ID:	113
Type:	basic
Owner:	admin
Label:	71cfa0de4981df28171710cf03332a99
Date Added:	2016-04-28 12:45:01 (UTC)
File Type:	PE32:win32:gui
File Size:	176128 bytes
MD5:	71cfa0de4981df28171710cf03332a99
SHA256:	50a5c41e0987d687a7cb83e8ae06d7f84489b8df0ea4c856add2a3fbcae8f246
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process:	C:\windows\temp\71cfa0de4981df28171710cf03332a99.exe ["C:\windows\temp\71cfa0de4981df28171710cf03332a99.exe"]

File System Events

Opens:	C:\Windows\Prefetch\71CFA0DE4981DF28171710CF03332-127E7825.pf
Opens:	C:\Windows
Opens:	C:\Windows\System32\wow64.dll
Opens:	C:\Windows\System32\wow64win.dll
Opens:	C:\Windows\System32\wow64cpu.dll
Opens:	C:\Windows\system32\wow64log.dll
Opens:	C:\Windows\SysWOW64
Opens:	C:\windows\temp\rvddshow2.dll
Opens:	C:\Windows\SysWOW64\rvddshow2.dll
Opens:	C:\Windows\system\rvddshow2.dll
Opens:	C:\Windows\rvddshow2.dll
Opens:	C:\Windows\SysWOW64\Wbem\rvddshow2.dll
Opens:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\rvddshow2.dll

Windows Registry Events

Opens key:	HKLM\software\microsoft\windows nt\currentversion\image file execution options
Opens key:	HKLM\system\currentcontrolset\control\session manager
Opens key:	HKLM\software\microsoft\wow64
Opens key:	HKLM\software\wow6432node\microsoft\windows nt\currentversion\image file execution options
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\wow6432node\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key:	HKCU\software\policies\microsoft\windows\safer\codeidentifiers
Queries value:	HKLM\software\microsoft\windows nt\currentversion\image file execution options[disableusermodecallbackfilter]

```
  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]
```