Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 215, Task ID: 861

Task ID:	861
Risk Level:	1
Date Processed:	2016-04-28 13:11:23 (UTC)
Processing Time:	2.27 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe"
Sample ID:	215
Type:	basic
Owner:	admin
Label:	af4ef1956ff0b59e9849a57d9fe16ec8
Date Added:	2016-04-28 12:45:12 (UTC)
File Type:	PE32:win32:gui
File Size:	69632 bytes
MD5:	af4ef1956ff0b59e9849a57d9fe16ec8
SHA256:	0c14ec6b8c51805eb948466868ffada2a0b25d9681032c257b5844d0b34f883c
Description:	None

Pattern Matching Results

Process/Thread Events

Creates process: C:\windows\temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe ["C:\windows\temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe"]
Terminates process: C:\Windows\Temp\af4ef1956ff0b59e9849a57d9fe16ec8.exe

File System Events

Opens: C:\Windows\Prefetch\AF4EF1956FF0B59E9849A57D9FE16-BF1122D2.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

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
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
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]
Queries value: HKLM\system\currentcontrolset\control\nls\sorting\versions[]