

# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 21, Task ID: 83

Task ID:	83
Risk Level:	1
Date Processed:	2016-04-28 12:48:49 (UTC)
Processing Time:	62.68 seconds
Virtual Environment:	IntelliVM
Execution Arguments:	"c:\windows\temp\19006d7d9c79190a3fb3032a97874a36.exe"
Sample ID:	21
Type:	basic
Owner:	admin
Label:	19006d7d9c79190a3fb3032a97874a36
Date Added:	2016-04-28 12:44:51 (UTC)
File Type:	PE32:win32:gui
File Size:	886168 bytes
MD5:	19006d7d9c79190a3fb3032a97874a36
SHA256:	0562a8ed75e8d1d36e4a342cf37f1281fbffb375c958d9f91638ab65fb975edb
Description:	None

## Pattern Matching Results

### Static Events

Anomaly: PE: Contains a virtual section

### Process/Thread Events

Creates process: C:\windows\temp\19006d7d9c79190a3fb3032a97874a36.exe  
["C:\windows\temp\19006d7d9c79190a3fb3032a97874a36.exe" ]

### File System Events

Opens: C:\Windows\Prefetch\19006D7D9C79190A3FB3032A97874-E782460F.pf  
Opens: C:\Windows\System32  
Opens: C:\windows\temp\mingwm10.dll  
Opens: C:\Windows\system32\mingwm10.dll  
Opens: C:\Windows\system\mingwm10.dll  
Opens: C:\Windows\mingwm10.dll  
Opens: C:\Windows\System32\Wbem\mingwm10.dll  
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\mingwm10.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]