# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 50, Task ID: 199

| | |
|---|---|
| Task ID: | 199 |
| Risk Level: | 4 |
| Date Processed: | 2016-04-28 12:52:26 (UTC) |
| Processing Time: | 61.27 seconds |
| Virtual Environment: | IntelliVM |
| Execution Arguments: | "c:\windows\temp\27c399c97ce41ca4b8add08cfeeb59b2.exe" |
| | |
| Sample ID: | 50 |
| Type: | basic |
| Owner: | admin |
| Label: | 27c399c97ce41ca4b8add08cfeeb59b2 |
| Date Added: | 2016-04-28 12:44:54 (UTC) |
| File Type: | PE32:win32:gui |
| File Size: | 91960 bytes |
| MD5: | 27c399c97ce41ca4b8add08cfeeb59b2 |
| SHA256: | a8306a2fa5ac6b6f7e50a3f073525d03c38ceeac53fe0f9884c2682e11e7bd9f |
| Description: | None |

## Pattern Matching Results

4 Checks whether debugger is present

## Process/Thread Events

Creates process: C:\windows\temp\27c399c97ce41ca4b8add08cfeeb59b2.exe ["C:\windows\temp\27c399c97ce41ca4b8add08cfeeb59b2.exe" ]

## File System Events

Opens: C:\Windows\Prefetch\27C399C97CE41CA4B8ADD08CFEEB5-86E7C903.pf
Opens: C:\Windows\System32
Opens: C:\windows\temp\RegisterLib.dll
Opens: C:\Windows\system32\RegisterLib.dll
Opens: C:\Windows\system\RegisterLib.dll
Opens: C:\Windows\RegisterLib.dll
Opens: C:\Windows\System32\Wbem\RegisterLib.dll
Opens: C:\Windows\System32\WindowsPowerShell\v1.0\RegisterLib.dll

## Windows Registry Events

Opens key: HKLM\system\currentcontrolset\control\session manager
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
Queries value: HKLM\system\currentcontrolset\control\session manager[cwdillegalindllsearch]
Queries value: HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]