# Malware Analysis Appliance by Blue Coat Systems, Inc.

## Task Details

Host: mag2, Sample ID: 50, Task ID: 198

| | |
|---|---|
| Task ID: | 198 |
| Risk Level: | 4 |
| Date Processed: | 2016-04-28 12:52:26 (UTC) |
| Processing Time: | 61.12 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\27C399C97CE41CA4B8ADD08CFEEB5-0810A226.pf
Opens: C:\Documents and Settings\Admin

## Windows Registry Events

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\27c399c97ce41ca4b8add08cfeeb59b2.exe
Opens key: HKLM\system\currentcontrolset\control\terminal server
Queries value: HKLM\system\currentcontrolset\control\terminal server[tsappcompat]