How to con your host?

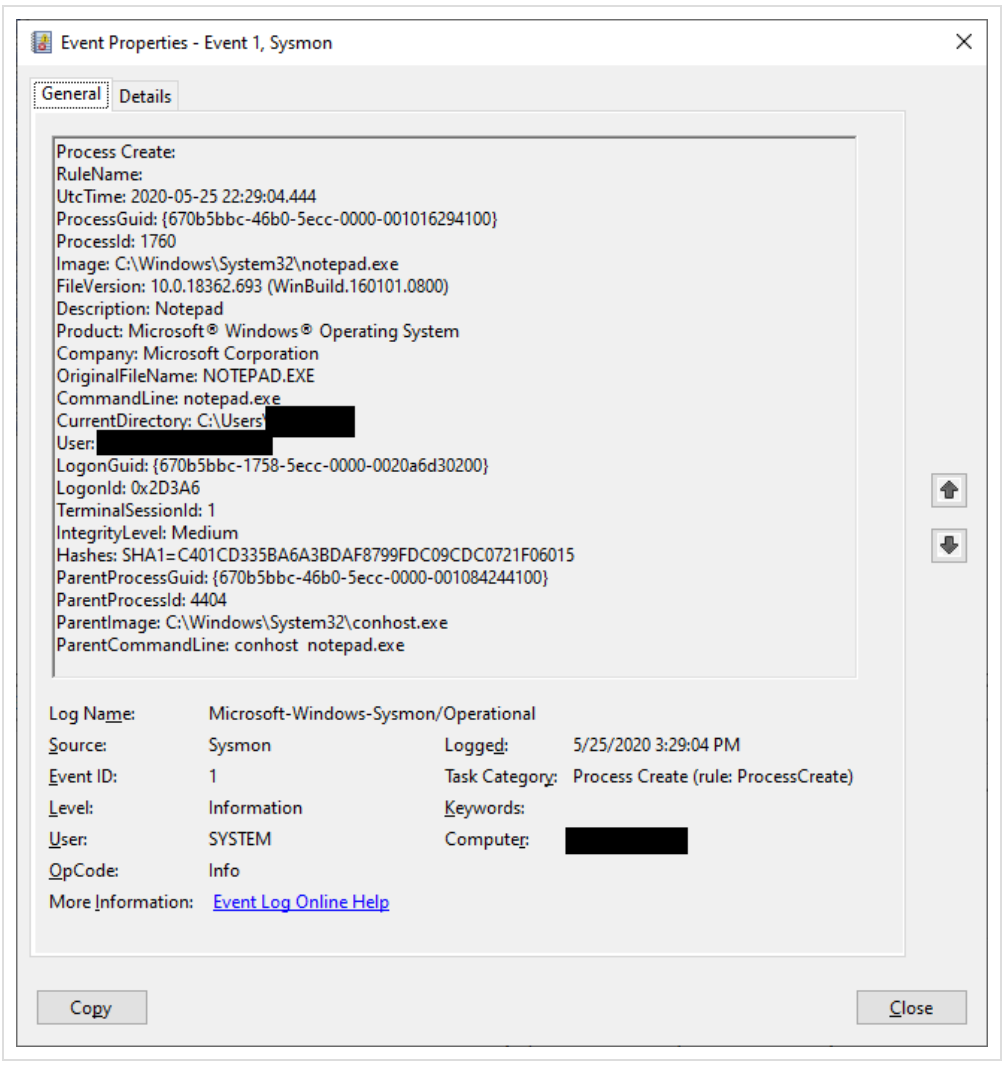
Good bye threat hunting configs and filters of the past. Microsoft introduced Windows Terminal and there is no way back.

While reading its actual source code today I noticed quite a lot of familiar code (I did poke around in conhost.exe code with Ida before), but then I stumbled upon an interesting bit that this post is all about.

The following command:

```
conhost.exe notepad.exe
```

doesn't do anything on older version of Windows 10. However, the latest version (tested on 18363) has a little LOLBINish surprise:



So… go back to your config and remove filters on *conhost.exe*. Remember, hate the message, not the messenger 😉

This entry was posted in **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.