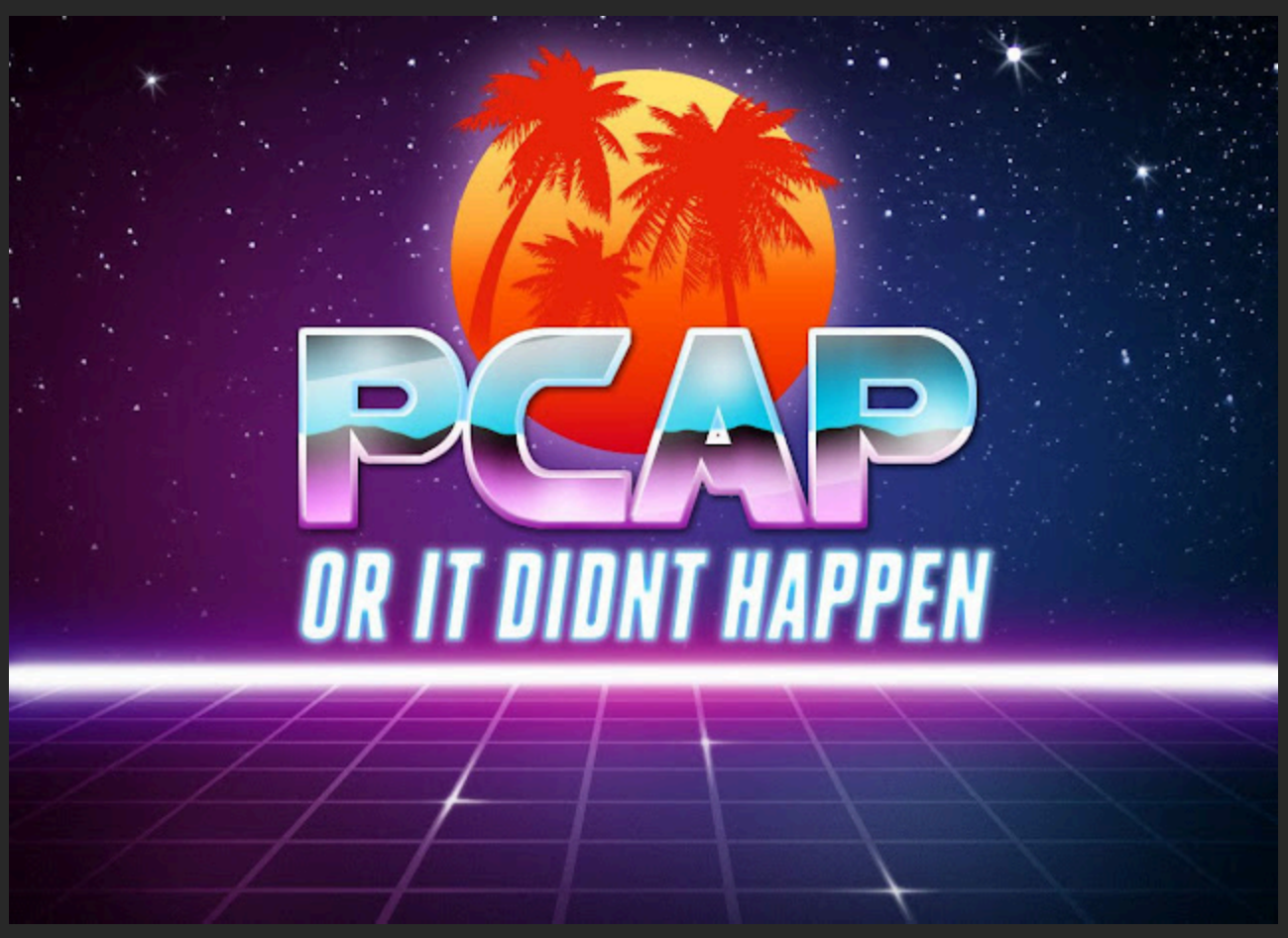
blue tangle

blue team dreams, splunk related detections and security insights. I poke around red team and threat actor tools and try to shed some light for cybersecurity wins.

Capturing Pcap driver installations

- June 10, 2020

Today we're looking at Network Sniffing, ATT&CK technique T1040.



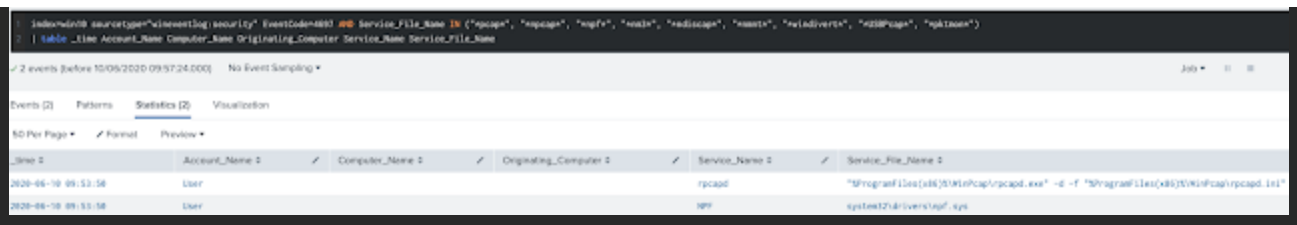
This is very much a signature based rule but if you are ingesting WinEventlog:Security (and of course you are, right?) and specifically EventCode 4697 ("A service was installed in the system") then you can take the barebones splunk SPL from below and make it work for you.

So how are we going to detect network sniffing on Windows endpoints? The installation of the drivers for the various Pcap variants.

```
index=win10 sourcetype="wineventlog:security" EventCode=4697 AND
Service_File_Name IN ("*pcap*", "*npcap*", "*npf*", "*nm3*",
"*ndiscap*", "*nmnt*", "*windivert*", "*USBPcap*", "*pktmon*")
| table _time Account_Name Computer_Name Originating_Computer
Service_Name Service_File_Name
```

The Service_File_Name list is derived from looking at the names of .sys files associated with the most popular packet capture options for Windows, it'll need to be kept up to date and less commonplace or renamed drivers may well slip through the net.

I installed AirPcap 4.1.3 and Win10Pcap on my test VM and both were caught by the above SPL.



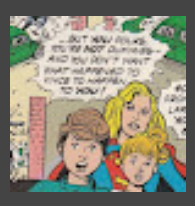
Happy hunting.

infosec security splunk windows

Popular posts from this blog

Fastening the Seatbelt on.. Threat Hunting for Seatbelt

- *August 26, 2022*



Quick blog entry on detections for the Ghostpack discovery/reconnaissance tool Seatbelt . This entry will focus on looking at command line parameters that can be caught even if the executable itself is renamed, if I have time we can delve into other event log artefacts another time. From the Seatbelt github repo: …

READ MORE »

Webshells automating reconnaissance gives us an easy detection win

- *July 22, 2020*

For those following along with ATT&CK this entry is about Server Software Component: Web Shell which is now a sub-technique of T1505, specifically it is T1505.003. If I can avoid combing through web access logs to find stuff like webshells I'll happily dodge it, having looked at the log artefacts left by a number of …

READ MORE »

Powered by Blogger