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.

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.

offensive and defensive security perspectives.

So essentially what the tool does is retrieve local system information that might have security or safety implications.

In terms of commands that can be tacked on to Seatbelt there are a literal ton of options.

But what we are going to focus on here are the command groups, which break the many, many available commands down into categories, so we have: `All, User, System, Slack, Chromium, Remote, Misc.`

The groups above are invoked like this, if you wanted to run all checks:

```
Seatbelt.exe -group=all
```

```
index=<winlogs-index> EventCode=4688 Process_Command_Line IN (*-group\=all, *-
group\=user, *-group\=system, *-group\=slack, *-group\=chromium, *-
group\=remote, *-group\=misc, *-outputfile\=\"*.json\", *-
outputfile\=\"*.txt\")

| stats min(_time) as earliest max(_time) as latest
values(Process_Command_Line) AS Process_Command_Line BY Account_Name
New_Process_Name ComputerName

| convert ctime(earliest) ctime(latest)

| table earliest latest ComputerName Account_Name New_Process_Name
Process_Command_Line
```

Please note the escaped "=" in the SPL and the liberal sprinkling of necessary asterisks.

You may get some false positives depending on how many programs you run that use a similar command line syntax to what I've outlined above, testing will be required in your environment.

If it works you wind up with something like this:

Happy hunting everyone.

ATT&CK command commandline cybersecurity Discovery elastic ghostpack Hacktool Invoke-Seatbelt lateral movement lockbit Lockbit Black ransomware seatbelt security splunk T1082 updates windows

---

Popular posts from this blog

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

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,

READ MORE »