ProcMon - Monitors Realtime activity
ProcExplorer - Show what processes are running and what DLLs have been loaded

Process Explorer and Process Manager together are great tools to use. ProcMon has great filtering tools that I can use.

- You can upload your currently running DLLs to virustotal through Process Explorer.
    - A virustotal box/tab shows up.
- You can have ProcessExplorer show whether or not running processes are verified.
- ProcMon has a great filtering tool where you can filter to only see .dll operations
- ProcMon can create legible Log Files where ProcessExplorer can create not-so-legible .txt files

The only method provided by microsoft to verify DLLs or .exe is the microsoft system file checker.

Use Virustotal to check for malicious or known DLLs

- Are usually identified by the PID or Process Name
    - With Sideloading/Hijacking, it is difficult to detect this kind of stuff

Any.run only had Windows 7 DLL examples.
It seems that a lot of research has been done on DLLs back in windows 7, and not much has been done since. This applies to any.run.

One way is to use SigCheck (built in feature) to make sure only legitimate processes are running

- SigCheck might be the best way

Another way is to look for unusual memory allocations or one process using more CPU usage (viewable in process explorer)

What the entire project could be: A constantly running (or choose when to run it) powershell script that causes ProcessExplorer to check for which processes are running, and to notify you of any that are running without a signature or verification. It can also notify you of any process that is using an unusual amount of CPU usage.

Powershell script: Shows actively running processes
Uploaded to GitHub
Any.run: Used process explorer to analyze Emotet malware, and could not find anything in Process Explorer. Emotet is known to use DLLs in a malicious manner.
I have saved my currently running processes as a baseline in a .txt file.

I ran Emotet on Windows 7 to attempt to look for DLL hijacking and I could not find anything. I will get a VM with Windows 11 and attempt to investigate from there.

Things I think I should do:

More research on Malware - try to see how malware affects DLLs in realtime?

DLL hijacking seems to be more popular.

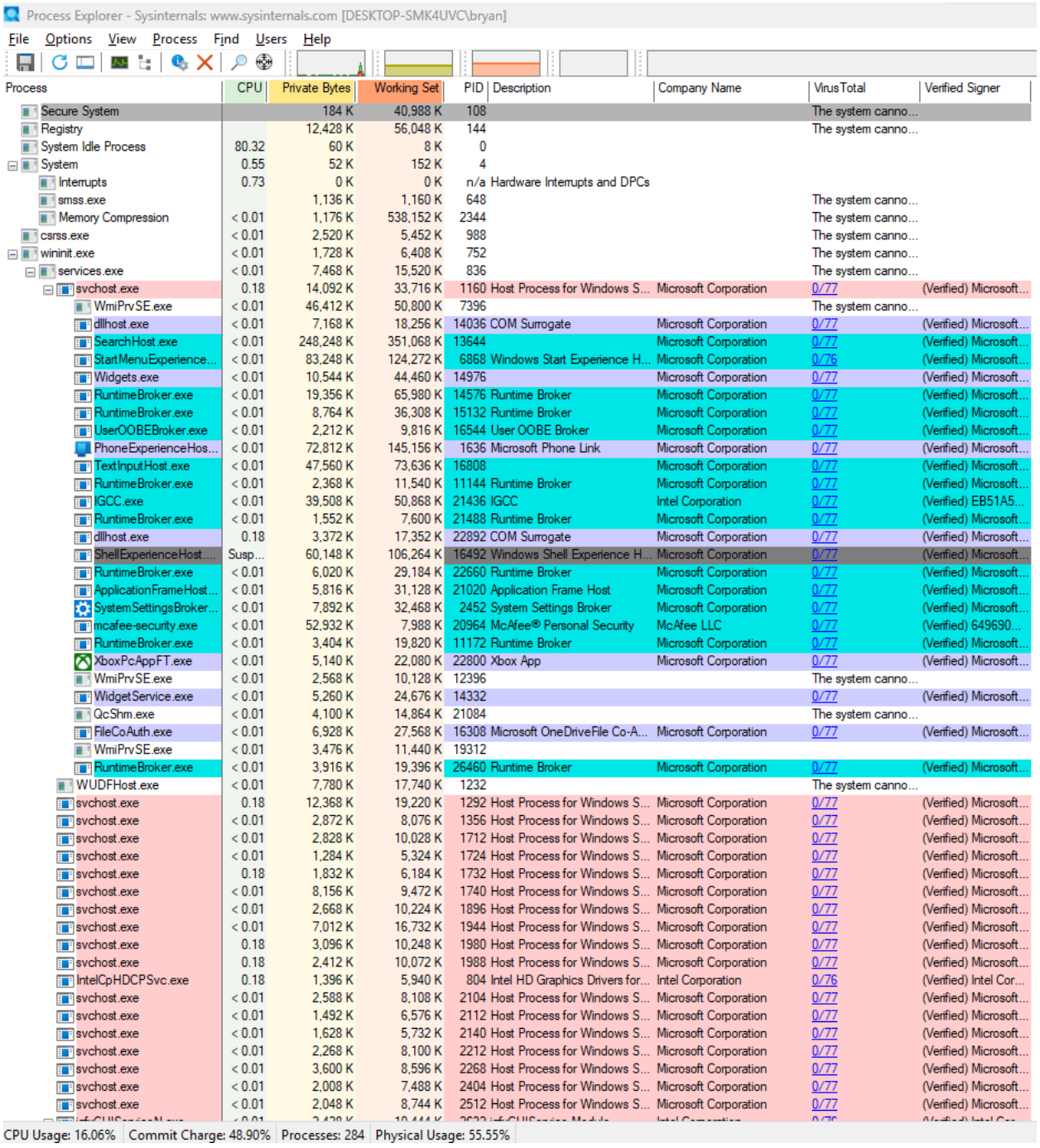
- Find a malicious DLL database
    - DLL hijacking will not really be able to be detected by this method

Get a working Windows VM - only have windows machine

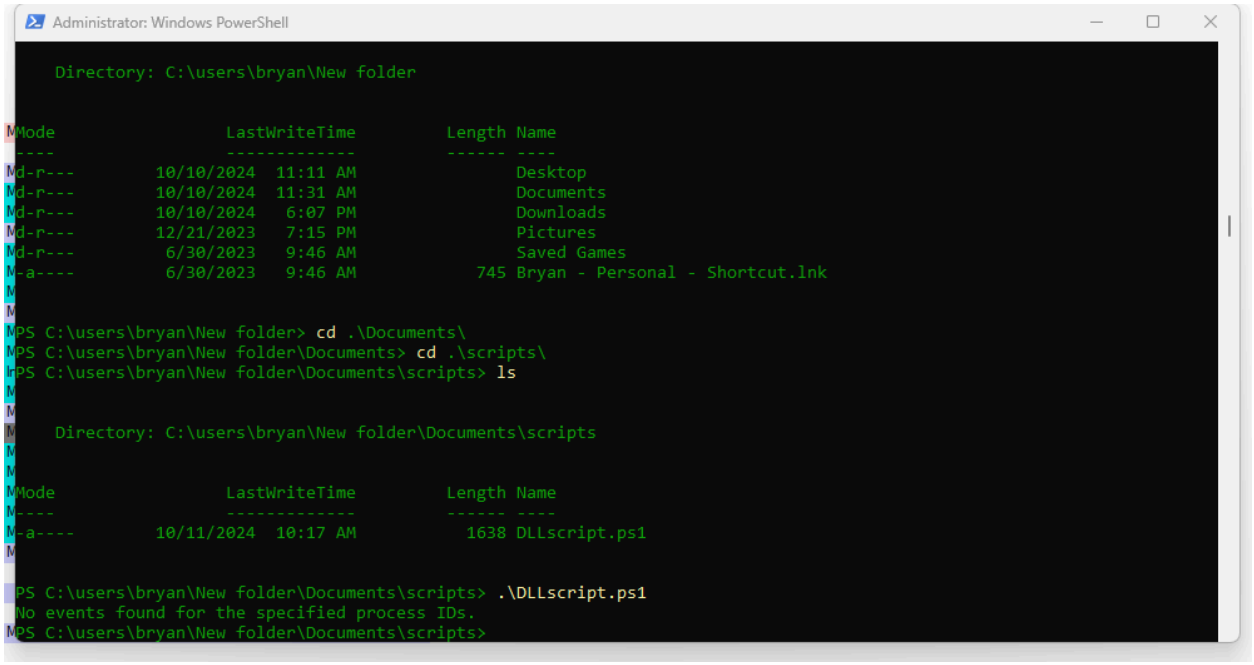
I found a Github project. It helps detect/prevent DLL sideloading, which is essentially the same as hijacking. https://github.com/XForceIR/SideLoadHunter

Stuff to do for next week:

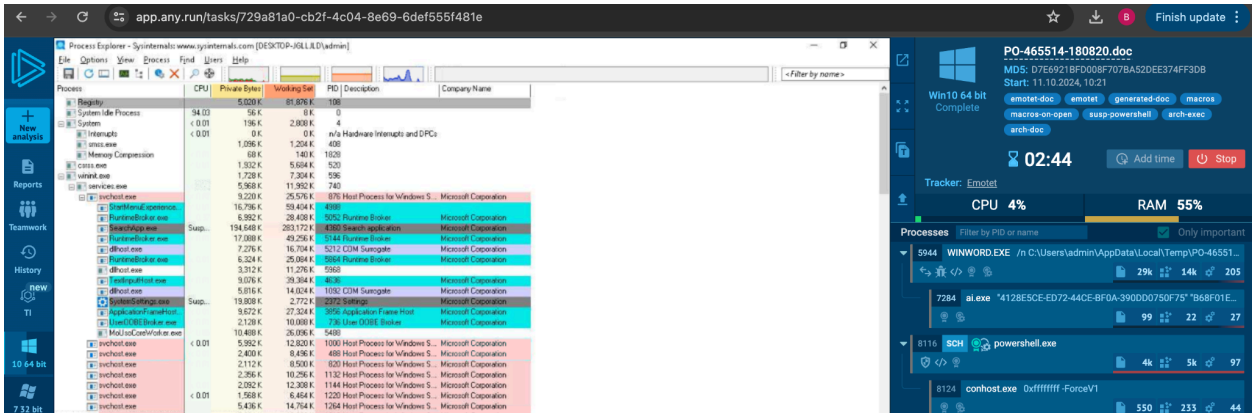
- Best way to track CPU and ram utilization on device
- Performance Monitoring tool built into windows
    - Set up baseline reports and be able to tell how much utilization each process uses on average, to identify baseline
    - This will allow you to identify any weird things going on
- Mostly using task manager
- Google cloud free tier for Windows 10/11
    - Mimic malware with intensive processes that use a lot of ram
- Focus on best way to track RAM and CPU utilization
    - Explain how microsoft/windows performance monitoring tool works (reports)
    - Look for additional tools



Process Explorer screenshot. Shows virustotal and verified signer.



Working powershell script (also on github).



Any.run malware analysis for emotet. Couldnt find much.