

- **Best way to track CPU and ram utilization on device**  
Windows Task manager for basic, and ProcMon for more in-depth analyzing of RAM utilization.
- Focus on best way to track RAM and CPU utilization
  - Explain how microsoft/windows performance monitoring tool works (reports)
  - Look for additional tools
  - The best tools are the ones that are already built into windows
    - Process Explorer both verifies signatures and works hand in hand with virustotal so thats two things i couldve done
    - ProcMon doesnt seem to be the best to use for finding malware
- **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
    - DONE
- **Google cloud free tier for Windows 10/11**
  - Got VM working - windows 10 - didnt do much on it
    - Should install some sort of malware or something on it (how)
- **SideLoader Github Project (Cloned on VSCode)**
- <https://github.com/XForceIR/SideLoadHunter>
- **(could not run, its not digitally signed)??**
  - SideLoader is a PowerShell script designed to detect DLL sideloading by analyzing executables and DLLs within user profiles, System32, and SysWow64 directories. The script profiles these files, compares their attributes (file names, hash values, internal names), and checks for DLL sideloading. It also examines program executions for sideloaded executables that are no longer present on the disk. (malware leaves a trace).
  - It does this by using: Get-SideLoadDetect: Identifies executables in userland directories with DLLs that match System32/SysWow64 names but are unsigned by Microsoft.
  - Get-SusShimcache: Analyzes ShimCache entries to detect sideloaded executables that have run from non-standard locations but no longer exist on disk.
  - Get-SusExec & Get-SusDLLs: Profiles the system to find System32 and SysWow64 executables and DLLs that are not in their default locations.

- After analysis, results are exported into CSV files, organized by hostname and date.

### How to proceed: (i think)

- Download malware on VM, see how it affects ProcExplorer/ProcMon, take note
- Compare vs baseline results
- Write script that analyzes and looks for what happens when malware is ran

### Screenshot of baseline process explorer

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-SMK4UVC\bryan]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal	Verified Signer
Secure System		184 K	40,988 K	108			The system cannot be reached	
Registry		12,428 K	56,048 K	144			The system cannot be reached	
System Idle Process	80.32	60 K	8 K	0				
System	0.55	52 K	152 K	4				
smss.exe	0.73	0 K	0 K	n/a	Hardware Interrupts and DPCs			
Memory Compression	< 0.01	1,136 K	1,160 K	648			The system cannot be reached	
csrss.exe	< 0.01	1,176 K	538,152 K	2344			The system cannot be reached	
wininit.exe	< 0.01	2,520 K	5,452 K	988			The system cannot be reached	
services.exe	< 0.01	1,728 K	6,408 K	752			The system cannot be reached	
svchost.exe	< 0.01	7,468 K	15,520 K	836			The system cannot be reached	
WmiPrvSE.exe	0.18	14,092 K	33,716 K	1160	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
dihost.exe	< 0.01	46,412 K	50,800 K	7396			The system cannot be reached	
SearchHost.exe	< 0.01	7,168 K	18,256 K	14036	COM Surrogate	Microsoft Corporation	0/77	(Verified) Microsoft...
StartMenuExperienceHost.exe	< 0.01	248,248 K	351,068 K	13644		Microsoft Corporation	0/77	(Verified) Microsoft...
Widgets.exe	< 0.01	83,248 K	124,272 K	6868	Windows Start Experience H...	Microsoft Corporation	0/76	(Verified) Microsoft...
RuntimeBroker.exe	< 0.01	10,544 K	44,460 K	14976		Microsoft Corporation	0/77	(Verified) Microsoft...
RuntimeBroker.exe	< 0.01	19,356 K	65,980 K	14576	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
RuntimeBroker.exe	< 0.01	8,764 K	36,308 K	15132	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
UserOOBEBroker.exe	< 0.01	2,212 K	9,816 K	16544	User OOBEBroker	Microsoft Corporation	0/77	(Verified) Microsoft...
PhoneExperienceHost.exe	< 0.01	72,812 K	145,156 K	1636	Microsoft Phone Link	Microsoft Corporation	0/77	(Verified) Microsoft...
TextInputHost.exe	< 0.01	47,560 K	73,636 K	16808		Microsoft Corporation	0/77	(Verified) Microsoft...
RuntimeBroker.exe	< 0.01	2,368 K	11,540 K	11144	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
IGCC.exe	< 0.01	39,508 K	50,868 K	21436	IGCC	Intel Corporation	0/77	(Verified) EB51A5...
RuntimeBroker.exe	< 0.01	1,552 K	7,600 K	21488	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
dihost.exe	0.18	3,372 K	17,352 K	22892	COM Surrogate	Microsoft Corporation	0/77	(Verified) Microsoft...
ShellExperienceHost.exe	Susp...	60,148 K	106,264 K	16492	Windows Shell Experience H...	Microsoft Corporation	0/77	(Verified) Microsoft...
RuntimeBroker.exe	< 0.01	6,020 K	29,184 K	22660	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
ApplicationFrameHost.exe	< 0.01	5,816 K	31,128 K	21020	Application Frame Host	Microsoft Corporation	0/77	(Verified) Microsoft...
SystemSettingsBroker.exe	< 0.01	7,892 K	32,468 K	2452	System Settings Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
McAfee-security.exe	< 0.01	52,932 K	7,988 K	20964	McAfee Personal Security	McAfee LLC	0/77	(Verified) 649690...
RuntimeBroker.exe	< 0.01	3,404 K	19,820 K	11172	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
XboxPcAppFT.exe	< 0.01	5,140 K	22,080 K	22800	Xbox App	Microsoft Corporation	0/77	(Verified) Microsoft...
WmiPrvSE.exe	< 0.01	2,568 K	10,128 K	12396			The system cannot be reached	
WidgetService.exe	< 0.01	5,260 K	24,676 K	14332			0/77	(Verified) Microsoft...
QcShm.exe	< 0.01	4,100 K	14,864 K	21084			The system cannot be reached	
FileCoAuth.exe	< 0.01	6,928 K	27,568 K	16308	Microsoft OneDriveFile Co-A...	Microsoft Corporation	0/77	(Verified) Microsoft...
WmiPrvSE.exe	< 0.01	3,476 K	11,440 K	19312				
RuntimeBroker.exe	< 0.01	3,916 K	19,396 K	26460	Runtime Broker	Microsoft Corporation	0/77	(Verified) Microsoft...
WUDFHost.exe	< 0.01	7,780 K	17,740 K	1232			The system cannot be reached	
svchost.exe	0.18	12,368 K	19,220 K	1292	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,872 K	8,076 K	1396	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,828 K	10,028 K	1712	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	1,284 K	5,324 K	1724	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	0.18	1,832 K	6,184 K	1732	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	8,156 K	9,472 K	1740	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,668 K	10,224 K	1896	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	7,012 K	16,732 K	1944	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	0.18	3,096 K	10,248 K	1980	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	0.18	2,412 K	10,072 K	1988	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
IntelCpHDCPSvc.exe	0.18	1,396 K	5,940 K	804	Intel HD Graphics Drivers for...	Intel Corporation	0/76	(Verified) Intel Cor...
svchost.exe	< 0.01	2,588 K	8,108 K	2104	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	1,492 K	6,576 K	2112	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	1,628 K	5,732 K	2140	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,268 K	8,100 K	2212	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	3,600 K	8,596 K	2268	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,008 K	7,488 K	2404	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,048 K	8,744 K	2512	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
svchost.exe	< 0.01	2,420 K	10,444 K	2620	Host Process for Windows S...	Microsoft Corporation	0/76	(Verified) Intel Cor...

CPU Usage: 16.06% | Commit Charge: 48.90% | Processes: 284 | Physical Usage: 55.55%