

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 Sideload/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 - Sysinternals: www.sysinternals.com [DESKTOP-SMK4UVC\bryan]

File Options View Process Find Users Help

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				
Interrupts	0.73	0 K	0 K	n/a	Hardware Interrupts and DPCs			
smss.exe		1,136 K	1,160 K	648			The system cannot be reached.	
Memory Compression	< 0.01	1,176 K	538,152 K	2344			The system cannot be reached.	
csrss.exe	< 0.01	2,520 K	5,452 K	988			The system cannot be reached.	
wininit.exe	< 0.01	1,728 K	6,408 K	752			The system cannot be reached.	
services.exe	< 0.01	7,468 K	15,520 K	836			The system cannot be reached.	
svchost.exe	0.18	14,092 K	33,716 K	1160	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...
WmiPrivSE.exe	< 0.01	46,412 K	50,800 K	7396			The system cannot be reached.	
dllhost.exe	< 0.01	7,168 K	18,256 K	14036	COM Surrogate	Microsoft Corporation	0/77	(Verified) Microsoft...
SearchHost.exe	< 0.01	248,248 K	351,068 K	13644		Microsoft Corporation	0/77	(Verified) Microsoft...
StartMenuExperienceHost.exe	< 0.01	83,248 K	124,272 K	6868	Windows Start Experience H...	Microsoft Corporation	0/76	(Verified) Microsoft...
Widgets.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	16356	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...
dllhost.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...
WmiPrivSE.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...
WmiPrivSE.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	1356	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	2,436 K	10,444 K	2632	Host Process for Windows S...	Microsoft Corporation	0/77	(Verified) Microsoft...

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

Process Explorer screenshot. Shows virustotal and verified signer.

```
Administrator: Windows PowerShell

Directory: C:\users\bryan\New folder

Mode                LastWriteTime         Length Name
----                -
d-r-----         10/10/2024 11:11 AM             Desktop
d-r-----         10/10/2024 11:31 AM             Documents
d-r-----         10/10/2024  6:07 PM             Downloads
d-r-----        12/21/2023  7:15 PM             Pictures
d-r-----         6/30/2023  9:46 AM             Saved Games
-a-----         6/30/2023  9:46 AM             745 Bryan - Personal - Shortcut.lnk

PS C:\users\bryan\New folder> cd .\Documents\
PS C:\users\bryan\New folder\Documents> cd .\scripts\
PS C:\users\bryan\New folder\Documents\scripts> ls

Directory: C:\users\bryan\New folder\Documents\scripts

Mode                LastWriteTime         Length Name
----                -
-a-----        10/11/2024 10:17 AM             1638 DLLscript.ps1

PS C:\users\bryan\New folder\Documents\scripts> .DLLscript.ps1
No events found for the specified process IDs.
PS C:\users\bryan\New folder\Documents\scripts>
```

Working powershell script (also on github).

The screenshot displays the Any.run malware analysis interface. The top section shows the sample name "PO-465514-180820.doc" and its MD5 hash. The left sidebar contains navigation options like "New analysis", "Reports", "Teamwork", "History", "TI", "10 64 bit", "732 bit", "Profile", "Pricing", "Contacts", "FAQ", "Log Out", and "FILES". The main area is divided into several panels: "Process Explorer" showing a list of running processes with columns for CPU, Private Bytes, Working Set, PID, and Description; "Network Requests" showing a list of HTTP requests with columns for TimeShift, Headers, Rep, PID, Process name, CN, URL, and Content; "System Information" showing details about the operating system, hardware, and software; and "Processes" showing a list of running processes with columns for PID, Name, and Description. The bottom status bar indicates "FREE trial" and "Warning: [5740] procexp64.exe Drops a system driver (possible attempt to evade defenses)".

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