**Analyzing a Reverse Shell Part 2\_Parent-Child Process Analysis**

# Executive Summary

This analysis delves into the examination of a suspicious process, "Rat.Unknown2.exe," using the Procmon tool to understand its behavior and potential implications, particularly in the context of malware analysis.

Initially, a filter was set up in Procmon to isolate activities associated with "Rat.Unknown2.exe." Despite no visible activity upon applying the filter, further exploration revealed its parent-child relationship with "Explorer.exe" as the parent process. This relationship underscores the significance of tracking processes to understand the flow of actions initiated by malware.

Subsequent steps involved observing the process tree within Procmon, illustrating the hierarchical structure of processes spawned by "Rat.Unknown2.exe." Notably, executing commands from a command prompt resulted in the creation of child processes under "Rat.Unknown2.exe," demonstrating its role as the parent process.

To better examine related processes, a filter was configured based on the Parent Process ID (PID) of "Rat.Unknown2.exe." This filter allowed for focused monitoring of activities stemming from this specific parent process, enabling a more comprehensive analysis of associated actions.

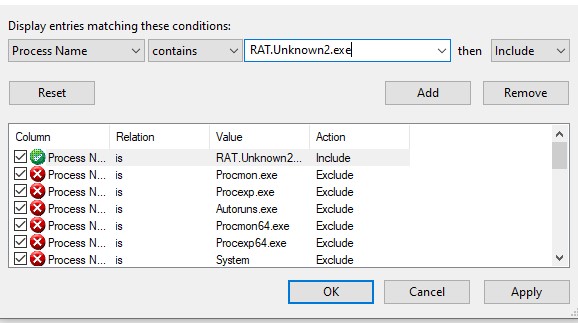
Ultimately, this investigation highlights the importance of understanding the parent-child process relationship in malware analysis. By visualizing process activity and tracing the origins of spawned processes, analysts gain valuable insights into the behavior and potential intentions of malicious software.

Overall, this analysis underscores the significance of leveraging tools like Procmon to dissect process behavior, enabling effective detection and mitigation of malware threats.

\*\*Parent-Child Relationship

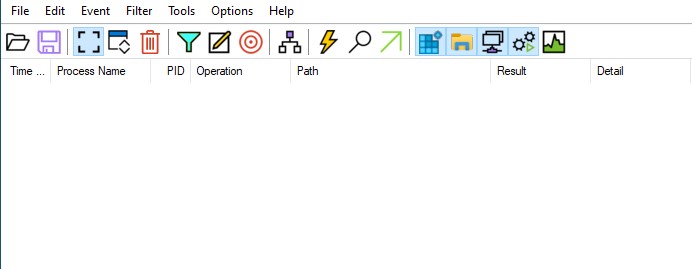
Let's pick up where we left off. Head back over to Procmon. Let's create the following Filter:

Process Name is Rat.Unknown2.exe



Make sure we click Add, followed by Apply, and finally OK.

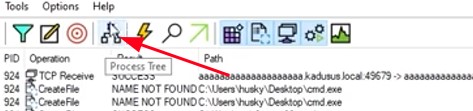
As we can tell, nothing populates thus far.



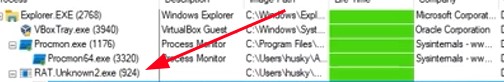
Head back over to CMDER, and run as admin. Type in "id" and we should see something populate inside of Procmon.

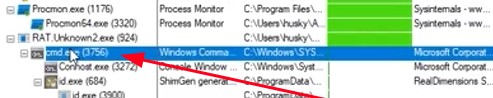


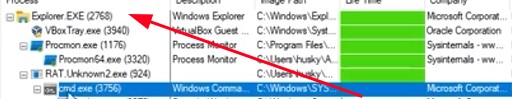
Let's go ahead and open the "Process Tree" inside of Procmon.



Lets navigate to Rat.Unknown2.exe.



Note, this process is actually a child process of Explorer EXE.



Basically, the parent is the process that executes and spawns all of the child processes. Therefore, anything that Rat.Unknown.exe does will be tied to its parent. The same applies to anything that branches off from Rat.Unknown2.exe.

Let's navigate back to CMDER and type in ipconfig. Then head back to the Process Tree. What has happened is that the main process Rat.Unknown2.exe is going to spawn a new process as it's child.

The information gathered thus far indicates that Rat.Unknown2.exe is the parent to cmd.exe below it. It is also spawning the other processes below it for cmd.exe. Malware authors will often try to break, or decouple the parent-child process relationship as much as possible.

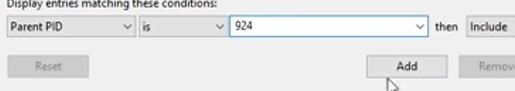
Process Tree is an excellent way to visualize what happens as a result of the main binary detonation (Malware). It will provide relevant information to inspect what the malware is doing.

Let's take note of the Parent ID (PID) for Rat.Unknown2.exe.



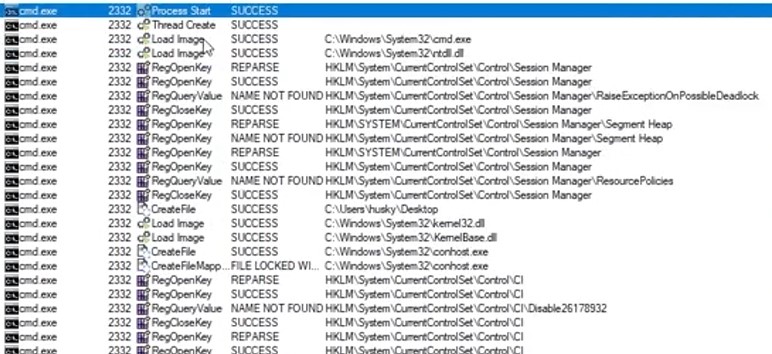
Head back to the Filter section inside of Procmon. Create the filter below:

Parent PID is 924



Click Add, then Apply, followed by OK.

Now everything that has Rat.unknown2.exe as it's parent process will be visible.



And there you have it. I hope this helps you understand the Parent-Child Relationship better when regarding malware. Thank you for your support.