Microsoft: Windows process launch

Windows process launch logs are a subset of security audit logs that track program activation, process exit, handle duplication, and indirect object access. You can audit successes or failures for each of these events. Furthermore, you can track how long a program was open and correlate the process data with logon events and object access events. Coupled with command line auditing, you can retrieve information regarding what commands were passed to open processes.

The most common events related to process launches are:

- 4688(S): A new process has been created.
- 4696(S): A primary token was assigned to process.

You can find other related events in the Microsoft documentation.

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Recommended index: oswinsec
- Source type: wineventlog:security
- Input type: WinEventLog://Security
- Add-on or app: Splunk Add-on for Microsoft Windows
- Sizing estimate: For Process Launch Logs (Event ID 4688), the expected volume can vary based on how many new processes spin up, but the variation is generally minor. Event ID 4688 is considered to provide excellent value in security logging. At a very high level, common ranges are:
  - Workstation: 4-6 MB/day (Including Application, System, and Security Logs)
  - Application Servers: 25-50 MB/day
  - Domain Controllers: 50-500 MB/day depending on the number of users

Validation

Usually the first thing people will see when deploying audit policies is either new systems showing up in Splunk, or at least an increase in system log messages. If you already have some logs coming in and want to validate that you’re getting the new ones, look for the delta between your old policy and your new one, and Google “Windows Event ID” – that will usually give you something specific to search for (though you may have to go take the action that gets logged, if it’s less common). An easy example is “Windows Process Creation Event ID” which quickly nets you “Event ID 4688” as
Application

When your Splunk deployment is ingesting Windows process launch logs, you can use the data to achieve the following:

- Detecting the use of randomization in cyberattacks
- Investigating a ransomware attack
- Recognizing improper use of system administration tools
- Detecting Netsh attacks

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.