Threat Hunting with Splunk

Introduction

In this project, I demonstrate my ability to perform threat hunting using Splunk by uncovering a command-and-control (C2) communication incident. A security alert flagged a suspicious file with an anomalous extension. My task was to investigate, pivot through Splunk logs, and uncover related adversary activities.

Step 1: Initial Process Execution Review

I started by filtering on process creation events (EventID=1) within the Sysmon logs (source=sysmon.json). My goal was to identify unusual process executions. I looked for abnormal file extensions or suspicious executables.

Step 2: Identifying the Suspicious File

I discovered an executable named application_form.pdf.exe. The double-extension stood out as a red flag. Switching to file creation events (EventID=11) confirmed when the file was created and where it resided.

Step 3: Tracking the File Download Source

I pivoted to file download events (EventID=22) to determine the file's origin. By also checking Edge process executions, I connected the malicious file download back to the msedge.exe process.

Step 4: Uncovering the C2 Communication

To validate C2 activity, I filtered on network connection events (EventID=3). I identified HTTP traffic to 13.232.55.12:8080. This confirmed the suspicious process was reaching out to an external command-and-control server.

Step 5: Investigating Attacker Commands

Next, I searched for cmd.exe executions. I found that the malicious process spawned a command prompt session. The attacker first ran 'whoami' to check privileges, followed by 'tasklist' to enumerate processes.

Step 6: Persistence via New User Account

Filtering for net.exe events revealed a command adding a new user account with a username and password. This confirmed the attacker established persistence.

Step 7: PowerShell Activity

I identified a PowerShell execution with the -ExecutionPolicy Bypass flag. This demonstrated the attacker bypassed execution policies to run malicious scripts.

Step 8: Firewall Rule Modification

Finally, I reviewed firewall policy logs. A new rule was added, indicating the administrator intervened to block malicious traffic and stop further attacker activity.

Summary

Through systematic filtering of Sysmon logs in Splunk, I was able to identify a suspicious file, trace its download origin, confirm C2 communication, observe attacker commands, detect persistence, uncover PowerShell bypass attempts, and validate defensive actions. This demonstrates my ability to investigate, correlate, and narrate attacker activity in a SOC environment.