Incident Detection and Response

December 21, 2023

Introduction

Part of the job we do as security analyst is monitoring and analyzing alerts, and responding to security incidents. In this project, I will be filling in for Jacqui, a colleague at Yoyodyne's satellite office in Kalamazoo who is on vacation.

The Scenario

From: jacqui@kz.yoyodyne
To: you@hq.yoyodyne
Subject: hope this helps!
I found a network diagram for you. A couple years old, but mostly up-to-date!
I jotted down some notes on the usual incident handling processes, at least here in the KZ office.
I launched a honeypot earlier this week. I meant to exclude it from the alerts, but what are the chances that any bad actors would have found it already?
Sorry I did not have time to put together more info! Good luck!
-j

Here is the project outline:

Outline

- Analyze Alerts from the Intrusion Detection System using Sguil.
- Live Packet Capture with tcpdump
- Read and Analyze Packet Captures with wireshark
- Create a Snort rule
- Use Splunk to Collect and Analyze Data
- Use Incident Response playbooks to Determine the Next Steps

1 IDS Alert Analysis using SGUIL via Security Onion

First analyzing a PCAP file that captured network alerts based on the snort rule written by Jacqui.

- Import PCAP file into Security Onion via terminal using the command.
  `sudo so-import-pcap`
- Open Sguil and login with your credentials to view imported network traffic.

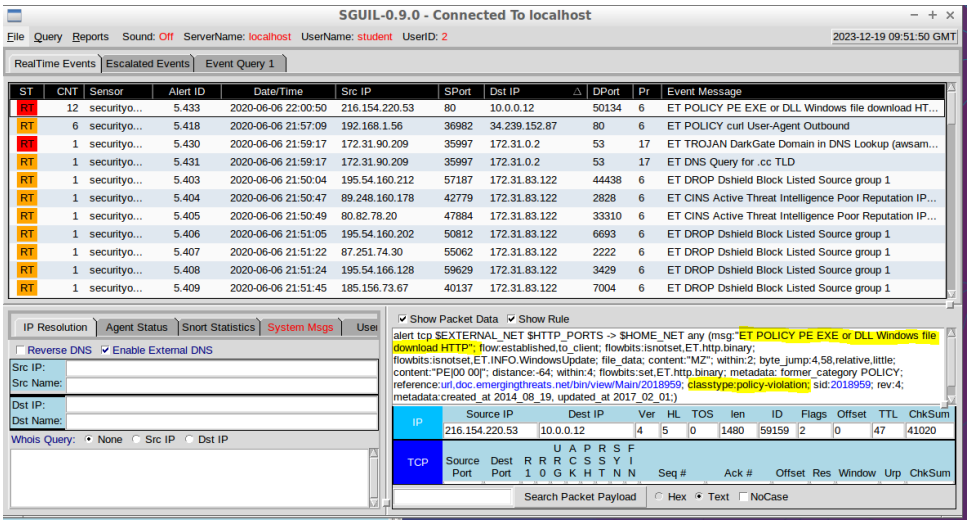

Figure 1: Reviewing Imported Network Traffic in Sguil

The first alert "ET POLICY PE EXE or DLL Windows file download HTTP", is suspicious.

2020-Jun-06 22:00:50 216.154.220.53:80 --> 10.0.0.12:50134

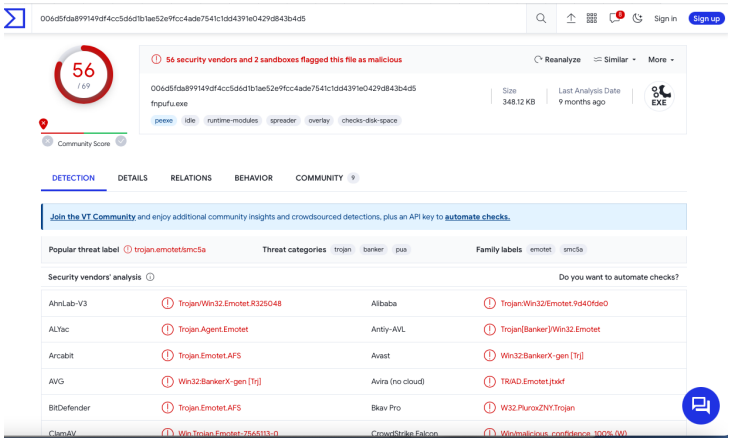

Figure 2: Result on VirusTotal, shows the file is a malware Trojan Emotet AFS

Common indicators are:

- alert of classtype policy-violation, which is of high priority.
- Downloaded malware named fnpufu.exe, the request made with an unusual user-agent.

The Source IP "216.154.220.53" shows no suspicious indication on VirusTotal. Further analysis include

- Download the payload fnpufu.exe and calculate the SHA256 using **sha256sum fnpufu.exe**
- Lookup the resulting file hash on VirusTotal.