Incident Handler's Journal – Entry #2

Lab Description:

In this lab, I used VirusTotal to check a file hash that came from a suspicious email attachment. The goal was to see if the file was actually malware and to find other indicators linked to it. I went through the VirusTotal report and pulled out the important details like detections, network connections, and related hashes.

Date: Record the date of the journal entry.	**Entry:** #2 **Date:** October 7, 2025
Description	I looked up the SHA256 hash in VirusTotal and reviewed the report to confirm if the file was malicious. I checked vendor results, community score, and related IoCs.
Tool(s) used	VirusTotal
Key Findings / Skills Practiced:	• 57 out of 72 vendors flagged the file as malicious. • Community score was -271, which shows it's not trusted. • File name: *bfsvc.exe*. • Tags in report: spreader, detect-debug-environment, runtime-modules, service-scan. • Practiced reading different tabs in VirusTotal (Detection, Details, Relations, Behavior).
Three IoCs (for Pyramid of Pain):	**Three IoCs (for Pyramid of Pain):** • **Hash value:** MD5 – `287d612e29b71c90aa54947313810a25`

	• **Domain name:** `a.sinkhole.yourtrap.com` • **IP address:** `104.115.151.81`
Decision — Is the file malicious?	Yes. Most vendors marked it as malware, and the community score backed that up. It clearly showed behavior tied to known trojans.
Additional notes:	I added one hash, one domain, and one IP to the Pyramid of Pain. VirusTotal made it easy to see how one file connects to a bunch of other malicious indicators.
