Incident handler's journal

Date: June 10, 2025	**Entry:** 2
Description	Performed a hash-based analysis of a suspicious file using VirusTotal. The goal was to determine whether the file was malicious based on antivirus vendor detection rates and community feedback.
Tool used	VirusTotal
The 5 W's	❖ **Who caused the incident?** Unknown — the file's origin is not yet identified, but it may have been created or distributed by a malicious actor (e.g., cybercriminal, threat group). ❖ **What happened?** A file was flagged by 59 out of 72 antivirus vendors on VirusTotal as malicious. The community score was strongly negative (-257), indicating high risk.

	❖ **When did the incident occur?** The investigation was conducted on 10 June 2025. The file's activity or detection date is not confirmed but likely predates the analysis. ❖ **Where did the incident happen?** The file was analyzed in a secure lab environment using VirusTotal. No indication yet of whether it was found on an endpoint or within an organization. ❖ **Why did the incident happen?** The file likely contains malicious code (e.g., trojan, backdoor, or spyware). It may have been shared via phishing, downloads, or removable media to gain access to an organization’s critical assets.
Additional notes	✚ The high detection ratio (59/72) and negative community score (-257) strongly suggest this file is dangerous. The file is classified as **malicious** based on overwhelming AV vendor detection and community feedback. It should be treated as a threat and **isolated, blocked, or deleted** if found on any system. ✚ Further analysis is recommended to understand the file’s behavior (e.g., static/dynamic analysis). ✚ Preventive action should be taken if this file is found in any network or device, including quarantine and alerting endpoint protection systems. ✚ Recommend adding this hash to internal threat intelligence databases.