Incident handler's journal

Date: 03-02-2001	Entry: 001 Initial response to suspicious file download triggered by IDS alert. File identified as malware via VirusTotal. Investigation in progress.
Description	An employee received an email containing a password-protected Excel spreadsheet. Upon opening the file using the password provided in the email, a malicious payload was executed. Multiple unauthorized executable files were created. The intrusion detection system flagged this behavior, and the SOC responded. The file's SHA256 hash (`54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b`) was submitted to VirusTotal, where it was confirmed to be malware (Flagpro/Fragtor family), associated with credential access, defense evasion, and persistence behaviors.
Tool(s) used	**VirusTotal**: For hash-based file analysis, malware family identification, IOC discovery **Intrusion Detection System (IDS)**: Detected unauthorized file creation **SIEM**: Alert triage and log correlation
The 5 W's	**Who** caused the incident? Likely a threat actor distributing malware through phishing emails; attribution unknown at this stage. **What** happened? A malicious spreadsheet file executed a payload upon opening, creating multiple unauthorized executables. **When** did the incident occur? Between 1:11 p.m. and 1:20 p.m.. **Where** did the incident happen? On an employee's workstation within the internal enterprise network. **Why** did the incident happen? .The employee opened a phishing email and accessed the file using the supplied password, triggering the malicious payload.
Additional notes	VirusTotal analysis showed 58/72 detection engines flagged the file as malicious. Behavioral tags included: `crypto`, `self-delete`, `runtime-modules`, `persistence`, `debug-evasion`. MITRE ATT&CK techniques observed: TA0005 (Defense Evasion), TA0006 (Credential Access), TA0003 (Persistence). Domains and IPs were extracted for blacklisting. Further actions: Threat hunting for lateral movement, domain/IP blocking, and user awareness reinforcement.