Date: 3/16/2024	**Entry: 2**
Description	Tracking security incidents, including the investigation and analysis of a suspicious file download leading to malware, using SHA256 hashing and VirusTotal for IoC discovery.
Tool(s) used	**VirusTotal website**
The 5 W's	Capture the 5 W's of an incident. • **Who caused the incident?** An employee received a suspicious email attachment. • **What happened?** The employee downloaded a password-protected spreadsheet and executed a malicious payload. • **When did the incident occur?** Timeline: 1:11 p.m. - Email received, 1:13 p.m. - File downloaded, 1:15 p.m. - Malicious program executed. • **Where did the incident happen?** On the employee's computer at the Financial service company. • **Why did the incident happen?** Due to the employee opening a malicious attachment from an email.
Additional notes	• The file hash has been reported as malicious by over 50 security vendors. • The file hash corresponds to the malware Flagpro. This is commonly used by the group BlackTech. • 57 out of 71 security vendors and 3 sandboxes flagged the file as malicious. • Threat labels include trojan.flagpro/fragtor, indicating a trojan malware family.