# Incident handler's journal

| | |
|---|---|
| **Date:** August 22, 2023 | **Entry:** #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None |
| The 5 W's | • **Who** caused the incident?<br>  ○ An organized group of unethical hackers known to target healthcare and transportation organizations<br>• **What** happened?<br>  ○ A ransomware incident<br>• **When** did the incident occur?<br>  ○ Tuesday at 9:00 a.m.<br>• **Where** did the incident happen?<br>  ○ A small U.S. health care clinic<br>• **Why** did the incident happen?<br>  ○ The hackers gained access to the company's network using targeted phishing emails sent to several employees. The emails contained a malicious attachment that installed malware to the employee's computer. After gaining access, the attackers deployed their ransomware, encrypting critical files and demanding money in exchange for the decryption key. This attack was most likely for financial gain. |
| Additional notes | More employee training on phishing attempts should be taught. Email filtering should also be implemented. Ensuring that critical files are properly backed up can mitigate the need for the decryption key. |

| **Date:**<br>August 24, 2023 | **Entry:** #2 |
|---|---|
| Description | Investigating a suspicious file hash |
| Tool(s) used | VirusTotal |
| The 5 W's | • **Who** caused the incident?<br>  ○ Unidentified malicious actor<br>• **What** happened?<br>  ○ An employee downloaded and opened a suspicious file with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b<br>• **When** did the incident occur?<br>  ○ Thursday at 1:11 p.m.<br>• **Where** did the incident happen?<br>  ○ Financial services company<br>• **Why** did the incident happen?<br>  ○ The employee received an email containing an attached, password-protected spreadsheet file. The employee downloaded the file and opened the spreadsheet using a password provided in the email. When the employee opened the file, a malicious payload was then executed on their computer. |
| Additional notes | Upon scanning the file's SHA256 hash on VirusTotal, it was determined that the file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech. Email filtering should be implemented as well as educating employees on suspicious emails. |