# Incident handler's journal

| | |
|---|---|
| **Date: 06/06/2023** | **Entry**: 1 |
| **Description** | This document highlights the danger posed on a Tuesday morning, at approximately 9:00 a.m by a group of hackers who use a type of malicious software (ransomware). |
| **Tool(s) used** | Tcpdump(packet sniffer), Wireshark(Packet Analyser) |
| **The 5 W's** | Capture the 5 W's of an incident.<br>● **Who** caused the incident?<br>A group of unethical hackers who are known to target organizations in healthcare and transportation industries<br>● **What** happened?<br>Phishing emails were dispatched to the personnel within the organization, whereby upon opening said emails, a pernicious program was instantaneously downloaded and proceeded to encrypt the organization's data. And a ransom note was left demanding a huge sum of money.<br>● **When** did the incident occur?<br>Tuesday morning, at approximately 9:00 a.m<br>● **Where** did the incident happen?<br>Inside the periphery of the company i:e within the company's Network<br>● **Why** did the incident happen?<br>The primary cause of the incident is currently under investigation; however, it appears that the opening of a phishing email is the fundamental catalyst behind the subsequent attack. |
| **Additional notes** | The organization had a disaster response plan in place, which helped streamline the incident handling process. All employees were notified of the incident and instructed not to use any affected systems until further notice. The IT team was quick to respond to the incident and worked closely with the incident handler to contain the attack and prevent |

| | |
|---|---|
| | data loss. The organization also hired a third-party cybersecurity firm to conduct an in-depth forensic investigation of the incident and to provide recommendations for improving their security posture. The incident highlights the importance of having robust cybersecurity measures in place to prevent such attacks and underscores the need for ongoing employee training and awareness programs to mitigate the risk of human error. |