**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** March 11, 2024 | **Emotet.exe** |
| Description | Analysis on Emotet malicious PCAP file |
| Tool(s) used | Wireshark |
| The 5 W's | * **Who**: An unethical virus called emotet * **What**: chain of events leading to an infection. Emotet is commonly distributed through malicious spam (malspam) emails. It was discovered to be banking Trojan. * **Where**: The incident occur at Tedprimehub’s outlet * **Why**: The incident must have occur because the server was not properly monitored. |
| Additional notes | 1. In order to prevent this incident from occurring again tedprimehub needs to keep monitoring their network always. 2. A security analyst need to always be in place so as not to allow incident like this from occurring again. 3. Firewalls, Wireshark, IDS should be also be installed |