|  |  |
| --- | --- |
| **Date**: 12th March, 2024 | **Entry**: Emotet malicious PCAP file |
| **Description**: | Analyzing Emotet.exe for Possible Malicious Activities |
| **Tool**(s): | VirtualBox, Kali Linux, Wireshark |
| **The 5 W’s** | **Who**: A process named Emotet.exe was running as root  **When**: Between the hours of 2:00hr and 5:00hr GMT+1  **Where**: This incident occurred in one of TedprimeHub’s outlet machine  **Why**: This attack must have been due to a discovered misconfigured server, after a successful infiltration. A command and Control (C2) server with the IP Address of 10.1.6.206 was exfiltrating company’s sensitive data through a compromised public server with the IP Address of 87.252.164.58, which then further exposed the internal network including IP Addresses 66.153.205.191, 173.255.195.246, 103.92.235.25 and 5.2.136.39 communicating with the C2 server.  **What**: This was discovered to be a Banking Trojan |
| **Recommendations**: | Security measures like Anti-Virus should be install and updated time to time. firewall and IDS/IPS should also be place and check.  Network monitoring should be done regularly, alongside with server and host reconfiguration. |