**INCIDENT REPORT: BN-18978-Malware-Traffic**

**Date: 6/19/2024**

**Executive Summary:** A friend reported their computer being encrypted after visiting websites offering free movie downloads. An analysis of the captured network traffic using Wireshark revealed three hostnames responsible for delivering the malware and identified the specific file used to execute it.

**Application Details:**

* Wireshark: Version 4.2.5
* PCAP File: Malware-Traffic.pcap

**Attack Narrative:**

1. **PCAP Analysis:** Opened the provided PCAP file in Wireshark to examine the network traffic.
2. **HTTP Traffic Filtering:** filtered out anything that didn't contain “This program” revealing 1 packet
3. **Extracting and Analyzing Files:** Extracted the suspicious files from the packet and uploaded it to VirusTotal for analysis.
4. **VirusTotal Confirmation:** VirusTotal confirmed that several of the files were malicious, including the file named "?b514ee6f0fe486009a6d83b035a4c0bd," which was likely the initial infection vector.
5. **Hostname Identification:** Identified the following three hostnames associated with the malicious traffic using VirusTotal:
   1. ip-addr.es
   2. comarksecurity.com
   3. static-ip-62-75-195-236.inaddr.ip-pool.com (62.75.195.236)

**Conclusion:**

The analysis indicates that the user's system was infected with malware delivered through malicious websites. The file "?b514ee6f0fe486009a6d83b035a4c0bd" was likely the initial executable that triggered the infection, leading to the download of additional malicious files and ultimately the encryption of the user's system. This incident highlights the importance of exercising caution when downloading files from untrusted sources.