**Incident Report: KG-19111-Defensive:-Erik’s-Coffee-Packet-Analysis  
Date:** 09-18-2024

### **Executive Summary**

In this task, I analyzed network traffic to identify two Windows hosts and determine which system was infected with malware. Using Wireshark, I discovered four GET requests for malicious files, extracted the SHA256 hash, and confirmed the presence of **Trojan.Qbot/Qakbot** via VirusTotal.

### **Methodology**

To complete this analysis, I followed these steps:

1. **Captured and Analyzed Network Traffic:**I used Wireshark to capture the network traffic, focusing on HTTP GET requests. Four GET requests to different domains were identified, all associated with the download of malicious files.
2. **Identified Windows Hosts and User Accounts:**The analysis revealed two Windows hosts:
   * **Elmer O'Brien** at **IP: 10.0.0.167**, MAC: **AC:16:2D** (Hewlett Packard)
   * **Alyssa Fitzgerald** at **IP: 10.0.0.149**, MAC: **6C:C2:17** (Hewlett Packard)
3. **Identified Four Malicious GET Requests:**I found four GET requests for the same malicious file, executed by **Elmer O'Brien’s** system (IP: 10.0.0.167), listed in chronological order:
   * **1st Request:** atn24live.com / **104.24.111.29** / **2020-04-23 23:18:32**
   * **2nd Request:** bg142.caliphs.my / **220.158.200.181** / **2020-04-23 23:18:33**
   * **3rd Request:** afsholdings.com.my / **220.158.200.181** / **2020-04-23 23:18:34**
   * **4th Request:** alphapioneer.com / **119.31.234.40** / **2020-04-23 23:18:35**
4. **Confirmed the Malware and Extracted the SHA256 Hash:**The downloaded file had a **SHA256 hash of f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1**. After submitting the hash to VirusTotal, it was confirmed to be **Trojan.Qbot/Qakbot** with a detection rate of 62/73.
5. **Malware Type:**The identified malware was **Trojan.Qbot/Qakbot**, a banking trojan capable of stealing sensitive information and enabling remote access to infected systems.

### **Findings/Solutions**

The infected machine belonged to **Elmer O'Brien** (IP: 10.0.0.167), who downloaded malicious files via four GET requests from the domains **atn24live.com**, **bg142.caliphs.my**, **afsholdings.com.my**, and **alphapioneer.com**. The **SHA256** hash confirmed the presence of **Trojan.Qbot/Qakbot**. To prevent future infections, I recommend stronger endpoint protection and user awareness training on the dangers of downloading files from untrusted websites.

**Project Description**

Erik’s business has been compromised with malware. He has contacted us and submitted logs. We know that he has two users who are hosts, and one of them got infected. He has no idea what the malware is or who could have brought it in. Analyze the packets and alerts he has sent us, then write a report to your Live Project Instructor with the following in it:

* Which two clients are Windows hosts, and what are the associated user account names?
* Which one of these two Windows clients was infected?
* What type of malware was that Windows client infected with?

Resources to look up malware:

* [https://www.cisecurity.org/resources/?type=white-papers%2f](https://www.cisecurity.org/resources/?type=white-papers/)
* <https://www.microsoft.com/en-us/wdsi/threats>

As per your first defensive story, find the folder with the matching name of this story, this will contain your PCAP for this story.

Be sure to write an incident report on your findings.