**INCIDENT REPORT: TS-18962-Defensive: Erik’s Coffee Packet Analysis**

**Date: 06/13/24**

**Executive summary:**

This User Story involves Erik’s Coffee, which has suffered a malware attack on one of two hosts. The malware and infected host is presently unidentified.

**Narrative:**

Using Wireshark, I was able to identify the Victim Details and IOCs while examining the included packets. Potential IOC’s were exported at HTTP Objects and uploaded to VirusTotal for analysis.

**Conclusion:**

The DESKTOP-GRIONXA host, which is assigned to user “elmer.obrien” was in communication with play.astrite.ga, a site whose country code belongs to Gabon in Central Africa. During this communication a zipped file containing the Qakbot Trojan was downloaded onto this device. The Qakbot Trojan is designed to steal financial information from the target system.

**Victim Details:**

* **Hostnames:**  DESKTOP-C10SKPY; DESKTOP-GRIONXA
* **IP Addresses:** 10.0.0.149; 10.0.0.167
* **MAC Addresses:** 6c:c2:17:f7:80:b6; ac:16:2d:f5:37:e5
* **Windows User Account Names:** alyssa.fitzgerald; elmer.obrien

**Indicators of compromise (IOCs):**

* **Malware Name/Type:** Qakbot Trojan, file: Judgement\_04222020\_318389448.zip
  + **IP Address:** 158.69.28.93
  + **Domain/URL:** play.astrite.ga
  + **SHA256 Hash:** 75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7