**Dataset**

* PCAP: **2021-09-20-TA551-BazarLoader.pcap**

**Queries Run**

* **Beaconing Detection**
* **Unusual Ports**
* **Exfiltration Attempts** (none found)
* **Mailspam Delivery** (none found)

**Findings**

* **Common IP**: 10.9.20.101
  + Seen in **beaconing** traffic
  + Also using **unusual ports**
  + Associated with **suspicious HTTP behavior**

**Correlation**

* The same internal host 10.9.20.101 was responsible for beaconing and using non-standard ports.
* No evidence of data exfiltration or mailspam in this PCAP.
* Suggests that this host is **compromised** and engaged in **C2 communication**.

**MITRE ATT&CK Mapping**

* **T1071 – Application Layer Protocol** (beaconing via HTTP/HTTPS)
* **T1095 – Non-Application Layer Protocol** (use of unusual ports)
* **T1059 – Command and Scripting Interpreter** (based on suspicious User-Agent patterns)