MITRE ATT&CK Mapping

Project 6 – Network Traffic Analysis (PCAP)

This document maps the **observed network behaviors** from the PCAP analysis to the **MITRE ATT&CK framework**. The mapping is based on DNS, HTTP, beaconing patterns, and suspicious IP communication identified using Wireshark.

---

1. Objective of MITRE Mapping

The purpose of this mapping is to:

- Translate raw network traffic findings into **adversary techniques**
- Demonstrate **threat-hunting and SOC analysis skills**
- Align the project with **real-world detection frameworks** used by blue teams

---

2. Observed Behaviors from PCAP

From Wireshark analysis:

- Repeated DNS queries to limited domains
- Short, periodic HTTP requests
- Communication with external IPs
- Traffic spikes at fixed intervals (beacon-like)
- Low data transfer with high frequency

---

3. MITRE ATT&CK Technique Mapping

◇ T1071 – Application Layer Protocol

Tactic: Command and Control

Evidence:

- HTTP requests observed using `http.request` filter
- Legitimate protocols used for suspicious communication

Why it matches: Attackers often use HTTP/HTTPS to blend C2 traffic with normal web traffic.

◇ T1071.004 – DNS

Tactic: Command and Control

Evidence:

- Multiple DNS queries from a single internal host
- Repeated resolution attempts to the same domains

Why it matches: DNS is commonly abused for:

- Beaconing
- Domain-based C2 resolution

◇ T1095 – Non-Application Layer Protocol

Tactic: Command and Control

Evidence:

- Raw IP communication observed between internal and external IPs

- Minimal payload exchange

Why it matches: Some malware avoids full application protocols to reduce detection.

◇ T1571 – Non-Standard Port

Tactic: Command and Control

Evidence:

- Communication occurring on uncommon or unexpected ports
- Traffic not aligned with normal service behavior

Why it matches: Non-standard ports help attackers evade simple firewall rules.

◇ T1046 – Network Service Discovery

Tactic: Discovery

Evidence:

- Short bursts of traffic to multiple IPs
- Low packet count per destination

Why it matches: May indicate automated probing or service enumeration.

◇ T1105 – Ingress Tool Transfer

Tactic: Command and Control

Evidence:

- HTTP communication potentially used to fetch payloads

- Small downloads observed

Why it matches: Attackers often use HTTP to download secondary stages.

---

4. Beaconing Behavior Mapping

◇ T1071 + T1059 (Indirect)

Observed Pattern:

- Regular time intervals between packets
- Consistent packet sizes
- Repeated destination IP/domain

MITRE Interpretation:

- Command-and-control beaconing
- Automated malware check-in behavior

---

5. Summary Table

Technique ID	Name	Tactic	Evidence
T1071	Application Layer Protocol	C2	HTTP requests
T1071.004	DNS	C2	Repeated DNS queries
T1095	Non-App Layer Protocol	C2	Raw IP traffic
T1571	Non-Standard Port	C2	Unusual ports
T1046	Network Service Discovery	Discovery	Multiple IP contacts
T1105	Ingress Tool Transfer	C2	HTTP downloads

---

6. SOC Analyst Perspective

From a SOC Level 1 viewpoint:

- Traffic should be escalated for **C2 investigation**
- DNS logs must be correlated with proxy/firewall logs
- Endpoint telemetry recommended for confirmation

---

7. Detection & Mitigation Suggestions

- Alert on **periodic DNS requests**
- Monitor **HTTP traffic with low payload but high frequency**
- Block known malicious IPs/domains
- Implement DNS logging and anomaly detection

---

8. Conclusion

This MITRE ATT&CK mapping demonstrates how **raw PCAP analysis** can be translated into **structured threat intelligence**. The observed behaviors strongly align with **Command-and-Control techniques**, reinforcing the value of Wireshark in SOC and malware traffic investigations.