MITRE ATT&CK; Mapping Report

Case: Suspicious DNS & HTTP Beaconing Activity
Analyst: Onur Tunç
Objective: Map observed attacker behaviors to the MITRE ATT&CK; framework based on PCAP analysis.

Tactic	Technique	Technique ID	Explanation
Command and Control	DNS	T1071.004	DNS used for command-and-control communicatio
Command and Control	Application Layer Protocol (HTTP)	T1071.001	HTTP GET requests used as beacon callbacks
Discovery	Network Service Discovery	T1046	Automated probing behavior to identify network se

Analyst Notes:
The mapping focuses on behavior-based analysis rather than signature detection. Techniques were selected based on traffic patterns, automation indicators, and communication characteristics observed in the PCAP.