Incident Response Mini Report

Incident Type: Suspicious DNS Beaconing Activity
Detection Method: Network Traffic & Log Analysis
Analyst: Onur Tunç

Detection

Suspicious repetitive DNS queries were detected during log and PCAP analysis, indicating potential automated beaconing behavior associated with command-and-control activity.

Containment

The affected endpoint would be isolated from the network to prevent further communication with external command-and-control servers.

Eradication

A full malware scan would be conducted, persistence mechanisms reviewed, and malicious artifacts removed from the system.

Recovery

The system would be restored to a clean state and monitored closely for any recurring suspicious activity.

Lessons Learned

DNS monitoring thresholds should be improved, and automated detection mechanisms should be enhanced to identify similar threats earlier.