DNS Tunneling Threat Hunt Report

Analyst

Abdulhaire

Date

April 15, 2025

Executive Summary

This threat hunting project investigates the presence of DNS tunneling, a covert method used by attackers to bypass network restrictions and exfiltrate data. Using packet capture (PCAP) analysis and the MITRE ATT&CK framework, encoded DNS queries were identified pointing to a suspicious domain, indicating the use of a DNS tunneling tool such as iodine. The goal of this project is to demonstrate the ability to detect hidden command-and-control (C2) channels through DNS traffic.

Tools Used

- Wireshark
- MITRE ATT&CK
- Base32 Decoder
- PCAP File: dns-tunnel-iodine.pcap

MITRE ATT&CK Mapping

Tactic: Command & Control

Technique: T1071.004 - Application Layer Protocol: DNS

Threat Discovery

Observations:

- Unusually long subdomain names detected in DNS queries
- Subdomains contain Base32-like encoded data
- Repeated destination domain: pirate.sea

- Communication occurs over UDP port 53

Wireshark Filter:

dns.qry.name.len > 15 && !mdns

Example Query:

7leaba82.2hb.Y.wgi...4yp1.C.t.I.y.pirate.sea

Stripped to: 7leaba822hbYwgi4yp1CtIy

Indicators of Compromise (IOCs)

- Suspicious Domain: *.pirate.sea
- Query Type: DNS A queries (type 1)
- Protocol: UDP/53
- Subdomain Pattern: Base32-style encoded strings

Impact

An adversary could use this tunnel to:

- Gain shell access to internal systems
- Exfiltrate sensitive data
- Maintain persistence and avoid detection

Detection Strategy

SOC teams can detect DNS tunneling by:

- Flagging DNS query names longer than typical (e.g., >60 chars)
- Detecting unusual query frequency to a single domain
- Monitoring for non-standard domain patterns (encoded subdomains)

Lessons Learned

- DNS tunneling is stealthy and easy to miss without deep inspection

DNS Tunneling Threat Hunt Report

- Wireshark is powerful for uncovering network-based covert channels
- Mapping findings to MITRE ATT&CK improves incident response workflows

Final Verdict

The analysis confirmed that the PCAP file contained DNS tunneling behavior using the iodine tool. This technique bypasses network policies and can be used for covert exfiltration or control.