Title: Detection of Command and Control (C2) Traffic via Uncommon TCP Port

Date: 21st May 2025

Analyst: Hanna Stambuli

Executive Summary

A suspicious TCP communication originating from an internal host was detected during a routine network analysis exercise using Wireshark. The internal device 10.5.12.22 was observed making persistent outbound connections to the external IP 176.65.144.169 over TCP port 7702, an uncommon and potentially malicious port. This traffic was indicative of possible Command and Control (C2) communication, prompting a full investigation.

Technical Findings

- Internal Host (Source IP): 10.5.12.22
- External Host (Destination IP): 176.65.144.169
- Source Port: 52275
- Destination Port: 7702
- Protocol: TCP

Indicators of Suspicion:

- Multiple persistent outbound connections
- Data in stream appeared encrypted or obfuscated
- No known legitimate services associated with port 7702

TCP Stream Behavior

Upon following the TCP stream, the data appeared unreadable, suggesting encryption or obfuscation consistent with malware beaconing or C2 communication. The internal host continued to reach out to the same IP across multiple sessions without receiving typical service responses indicating non-standard communication behavior.

Threat Intelligence & Correlation

- The IP 176.65.144.169 is associated with previously flagged C2 infrastructure in threat intelligence feeds (e.g., CleanTalk, Joe Sandbox).
- Destination Port 7702 is not associated with any known legitimate services and appears in malware related telemetry.
- The connection pattern matches behavior of Remote Access Trojans (RATs) or botnet beacons.
- Public sources showed historic behavior linked to malware payloads, script loaders, and spam operations.

Impact Analysis

Impacted Device: 10.5.12.22

Potential Impacts:

- Host compromise with possible remote control
- Data exfiltration
- Lateral movement risk within the internal network
- Risk of external command execution and internal persistence
- Use of the host as a pivot or relay in botnet campaigns

Immediate Actions & Recommendations

- Isolate the affected host from all networks immediately.
- Conduct a full forensic malware scan using AV and EDR solutions.
- Review endpoint and server logs for lateral movement or access attempts.
- Block all outbound communication to 176.65.144.169 and TCP port 7702 across perimeter firewalls.
- Investigate internal logs for any additional devices communicating with the malicious IP.
- Retain forensic logs, .pcap files, and communication traces for follow up analysis. Notify incident response or Tier 2 analysts and initiate triage procedures.