Wireshark Project Lab Report

TRAFFIC ANALYSIS EXERCISE: NEMOTODES

Objective

You work as an analyst at a Security Operation Center (SOC) for a medical research facility specializing in nemotodes. Alerts on traffic in your network indicate someone has been infected. You don't know which is more disgusting, the nemotodes or the malware.

Tools Used

- **Wireshark**
- **PCAP File:** http://2024-11-26-traffic-analysis-exercise.pcap.zip/ **(from ware-traffic-analysis.net)**

PCAP Summary

- **File Name:** http://2024-11-26-traffic-analysis-exercise.pcap.zip/
- **Description:** You work as an analyst at a Security Operation Center (SOC) for a medical research facility specializing in nemotodes. Alerts on traffic in your network indicate someone has been infected. You don't know which is more disgusting, the nemotodes or the malware.

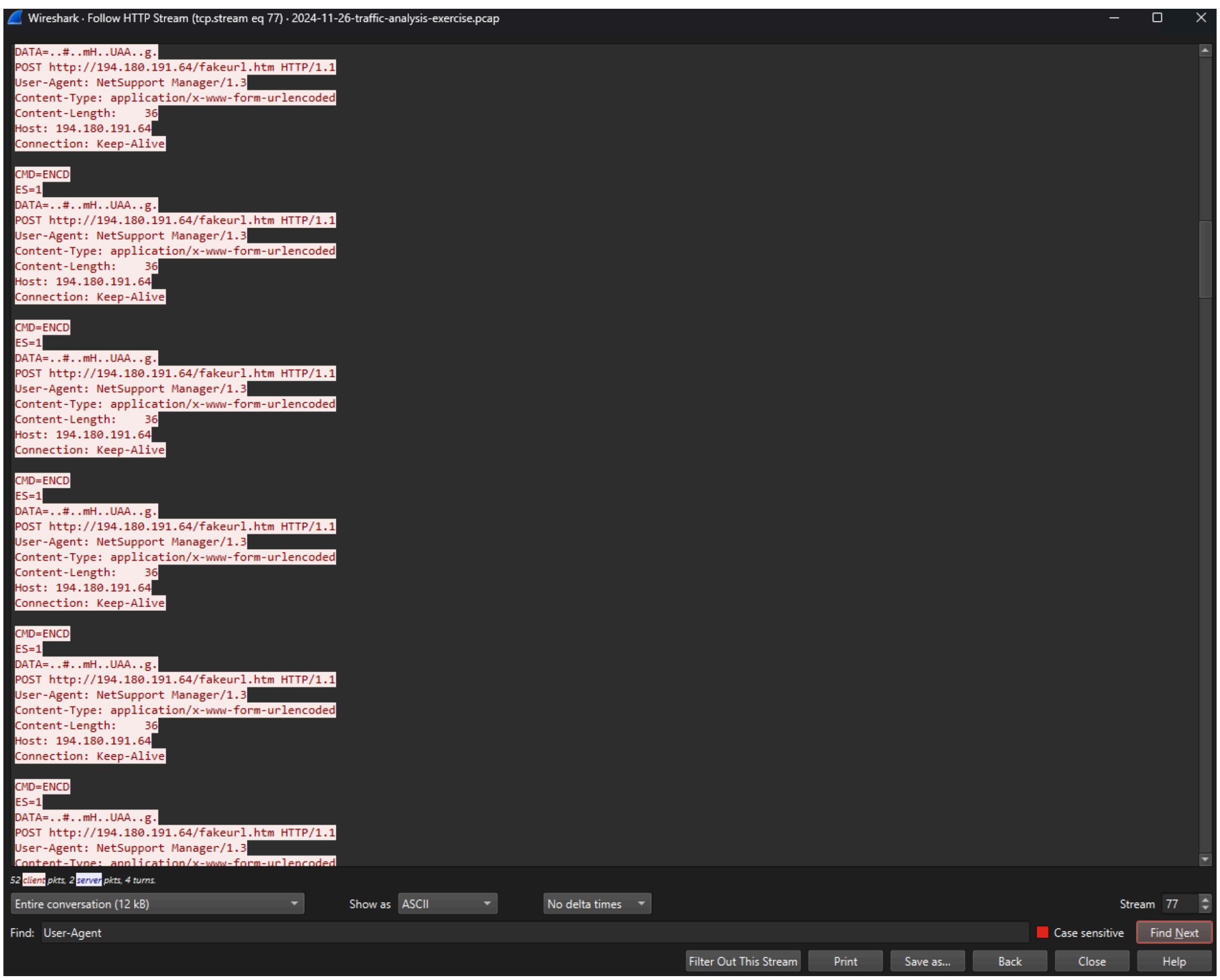
10.11.26.183 (internal ip) has high number requests to 193.42.38.139 .
13248 packets

Next I filtered by this command
ip.addr == 10.11.26.183 && ip.addr == 193.42.38.139 and there are 13238 packets displayed

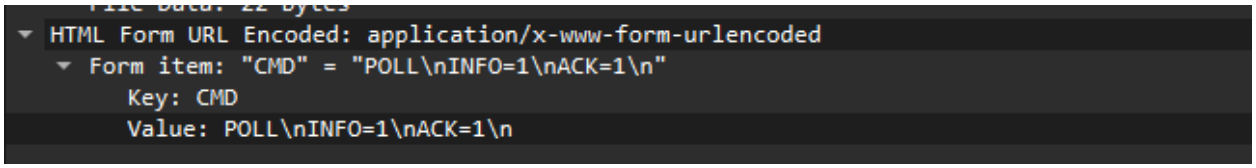
When applying the filter `http && ip.addr == 10.11.26.183`, I observed repeated HTTP traffic from **source IP 10.11.26.183** to **external IP 194.180.191.64**, which is also flagged in the alert sheet.

Among this traffic were multiple **POST requests** to `http://194.180.191.64/fakeurl.htm`, which appear suspicious. These requests use **"Connection: Keep-Alive"**, lack the **X-Forwarded-For** header, and specify a **User-Agent of NetSupport Manager/1.3** — a legitimate remote desktop tool often abused by threat actors as a **Remote Access Trojan (RAT)**.

This pattern suggests possible unauthorized remote access activity like a RAT



Upon analyzing the POST request for the fakeurl, I noticed that in the HTML Form URL Encoded



This looks like a **malicious command and control (C2)** communication, specifically a **polling request**

CMD: This is likely a command being sent to the server. The value `"POLL\nINFO=1\nACK=1\n"` indicates that the infected machine is sending a request to the command and control (C2) server.

POLL: This suggests that the infected machine is polling the C2 server for instructions.

INFO=1: This could be a flag indicating that the infected machine is reporting information back to the server, possibly about its status or environment (e.g., system information, IP address, etc.).

ACK=1: This likely indicates an acknowledgment of the server's last command or request, meaning the infected machine is confirming that it received something from the C2 server.

Incident Report

Executive Summary:

On November 26, 2024, a malicious actor exploited the network of a medical research facility specializing in nemotodes. The attacker initiated a malicious POST request to an internal server, using a fake URL to send suspicious commands. This activity involved communication with an external IP address, 194.180.191.64, which could indicate malware or Remote Access Trojan (RAT) activity. The nature of the request and the presence of NetSupport Manager in the User-Agent suggests that

the attacker was attempting to test the server's vulnerability to exploit further or gain unauthorized remote access to the system.

Victim Details:

Victim - 10.11.26.183
MAC Address - d0:57:7b:ce:fc:8b
DEVICE NAME DESKTOP-B8TQK49 ,
User account name - oboomwald

Indicators of Compromise (IOCs):
194.180.191.64 , http://194.180.191.64/fakeurl.htm , user-agent i see NetSupport Manager/1.3 which is a remote desktop software which could mean a RAT **, CMD: This is likely a command being sent to the server. The value `"POLL\nINFO=1\nACK=1\n"` indicates that the infected machine is sending a request to the command and control (C2) server.**