Group: Essential Group	Report Number: Report No. 9	Report id 9-lec-13-Detection&analysis using ids&ips suricata_7

Analyze the PCAP File

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed

Date of Task Assignment :

2/6/2026

Due Date:
2/10/2026

Contents

Introduction

This document outlines the comprehensive process of identifying, analyzing, and documenting the activities of a **Remote Access Trojan (RAT)** known as **STRRAT**, which was observed during an in-depth network traffic analysis. The investigation was centered around the infection of a system in the network, labeled **172.16.1.66**, which established communication with a Command and Control (C&C) server at **141.98.10.79**. This report includes a technical breakdown of the captured network traffic, key indicators of compromise (IOCs), and visual representations to demonstrate the flow of malicious activities.

1. Executive Summary

- **Incident Overview**: The incident involves a potential malware infection on the system with the hostname **DESKTOP-SKBR25F**. The infection appears to be associated with the **STRRAT** malware family, which is a type of Remote Access Trojan (RAT). It is engaging in **Command and Control (C&C) communication** with an external server (141.98.10.79).
- **Timeline**: The event occurred on **2024-07-30** between **02:38:48** and **02:41:43 UTC**.
- **Key Event**: The system was found initiating several outbound connections to an external IP address, believed to be controlled by the attacker. The malware uses **TCP port 12132** for communication, with a **STRRAT CnC Checkin** signature detected by Suricata.

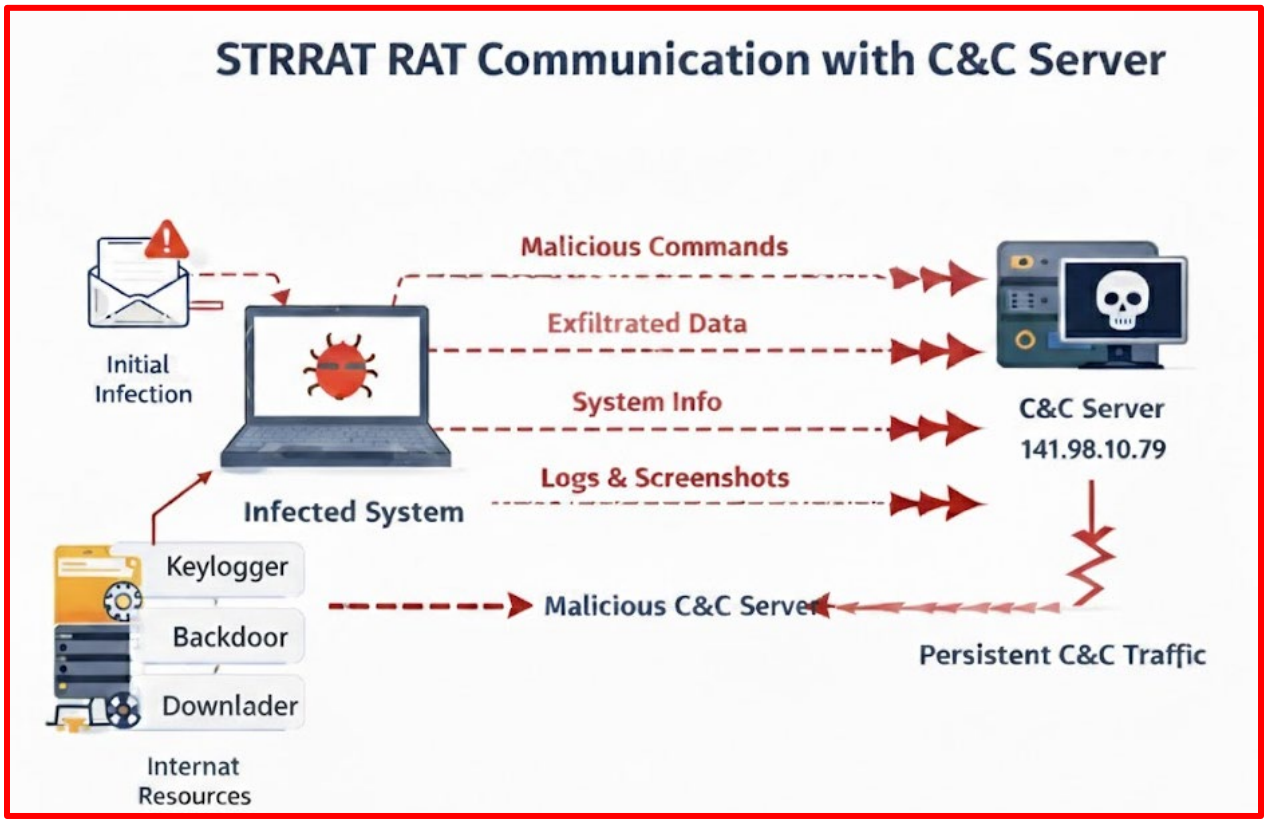


Figure (1) shows how **STRRAT** malware typically communicates with C&C servers.

2. Victim Details

- **Hostname**: **DESKTOP-SKBR25F**
- **IP Address**: **172.16.1.66**
- **MAC Address**: **00:1E:64:EC:F3:08**.
- **Windows User Account Name**: (N/A)
- **Additional Information**:
    - The infected system is attempting to resolve several domain names, including _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.wiresharkworkshop.online and wireshark-ws-dc.wiresharkworkshop.online, indicating possible communication with internal systems or domain controllers.
    - The system is engaged in **LDAP queries** and **DNS requests**, both of which are normal, but the repeated C&C communication suggests potential malicious activity.
- **System Activity:**
  The infected system was observed making frequent requests to the following services:
    - **Port 445 (SMB)**: Likely to exploit file sharing and possible lateral movement within the network.
    - **Port 389 (LDAP)**: Possible enumeration of users or devices on the network.
    - **Port 53 (DNS)**: Suspicious DNS traffic, possibly for tunneling or covert communication.
    - **Port 135 (RPC)**: Exploits RPC services, used for remote access or code execution.
    - **Port 443 (HTTPS)**: For encrypted communication to external malicious servers, potentially for exfiltration or command execution.
- **Internal Network Activity:**
    - The system attempted several network connections to internal services such as SMB and DNS, possibly searching for vulnerable machines or attempting data exfiltration.
    - A large portion of the traffic was sent out to external addresses over **HTTPS (Port 443)**, suggesting the use of encrypted exfiltration channel
- **Presence of Malware:**
    - STRRAT appears to have been successfully deployed, based on the consistent **C&C check-ins** and the traffic patterns seen across different ports.

- STRRAT may have been dropped by an initial exploit or phishing email targeting this host.

Traffic Analysis and Overview

To initiate the traffic analysis, Suricata was executed in offline mode using a custom bash script. This allowed Suricata to process a pre-captured PCAP file (traffic-analysis-exercise.pcap) without the need for live network traffic.

Figure (2) shows the script we used to run Suricata offline

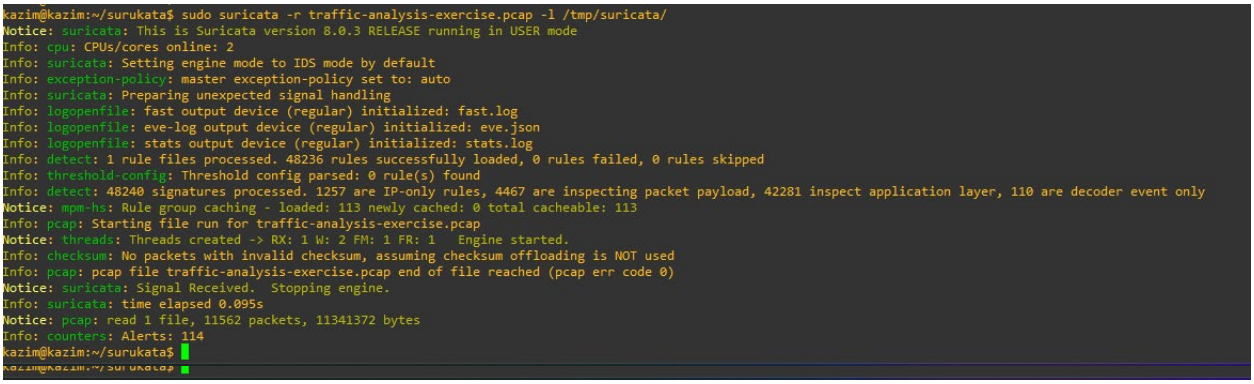


Figure (3) shows Suricata generated a total of **114 alerts**

The captured traffic and logs were meticulously analyzed using **Suricata** for patterns indicating **malicious C&C communications**. Several critical findings include:

3. DNS Query Log

A DNS query for wireshark-ws-dc.wiresharkworkshop.online was observed, confirming the **communication between the infected system** and the **domain controller** (172.16.1.4). The query and response logs revealed the active presence of a malicious entity attempting to identify **service records (SRV)**.

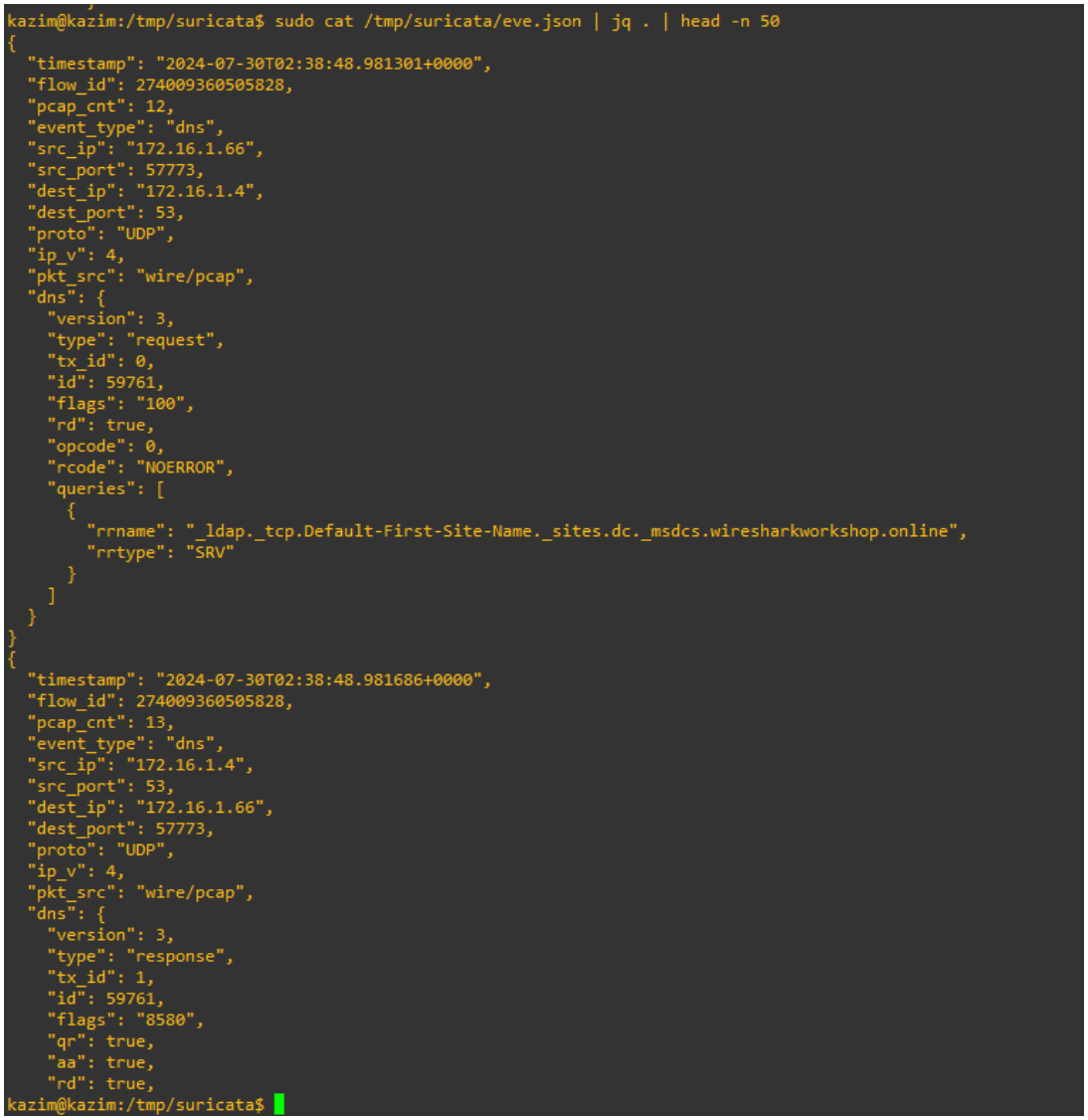


Figure (4) shows DNS Query Log

4. Indicators of Compromise (IOCs)

Suricata flagged multiple instances of **STRRAT C&C Check-ins**. Each check-in was detected as a **malware command and control activity** with the **signature "ET MALWARE STRRAT CnC Checkin"**.

Sample Suricata Alert:

- **Signature**: ET MALWARE STRRAT CnC Checkin
- **Alert ID**: 2030358
- **Severity**: Major
- **Detected Traffic**:
  - **Source IP**: 172.16.1.66 (infected system)
  - **Destination IP**: 141.98.10.79 (C&C server)
  - **Port**: 12132 (used for C&C traffic)

- **Malicious IP Address**: 141.98.10.79 – This is the external server involved in the C&C check-ins.
- **Malicious Domains**:
  - _ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.wiresharkworkshop.online
  - wireshark-ws-dc.wiresharkworkshop.online
- **Malware Family**: **STRRAT**
- **Ports**:
  - **TCP Port 12132** (Primary C&C communication port)
- **Suricata Signature**:
  - **ET MALWARE STRRAT CnC Checkin** – The signature for the **STRRAT** malware was triggered multiple times during the investigation.

5. Malicious Activity Detected

- The infected system (172.16.1.66) was observed sending multiple **STRRAT CnC check-ins** to the external server (141.98.10.79) using **TCP port 12132**. This indicates ongoing communication between the infected system and the attacker, which is characteristic of a **Remote Access Trojan** (RAT).
- **Malware Activity**:
  - **STRRAT** is being used to maintain control over the infected system and possibly exfiltrate data.
  - The infected system was engaging in **LDAP searches** and DNS queries, potentially to map out the internal network or gain additional credentials.

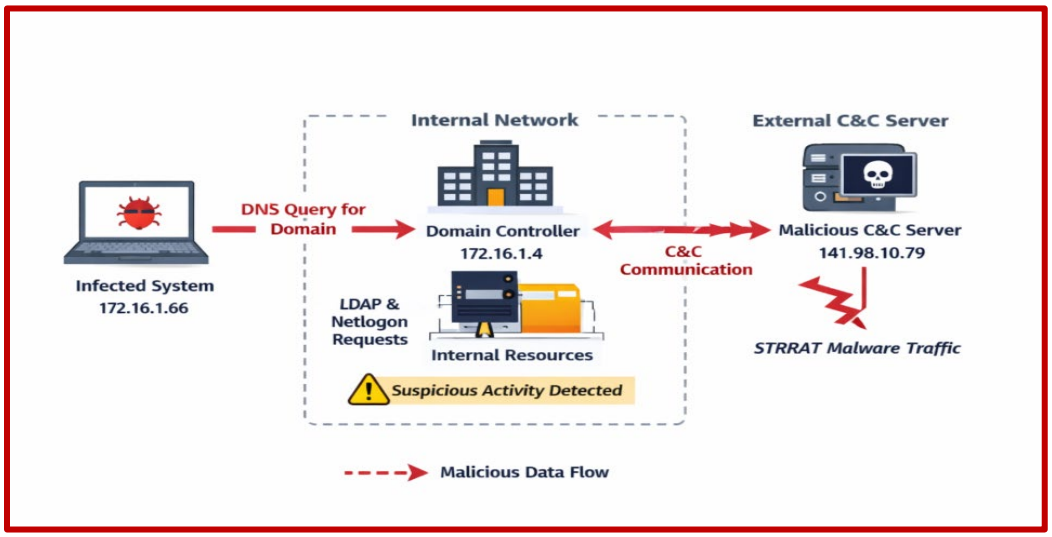
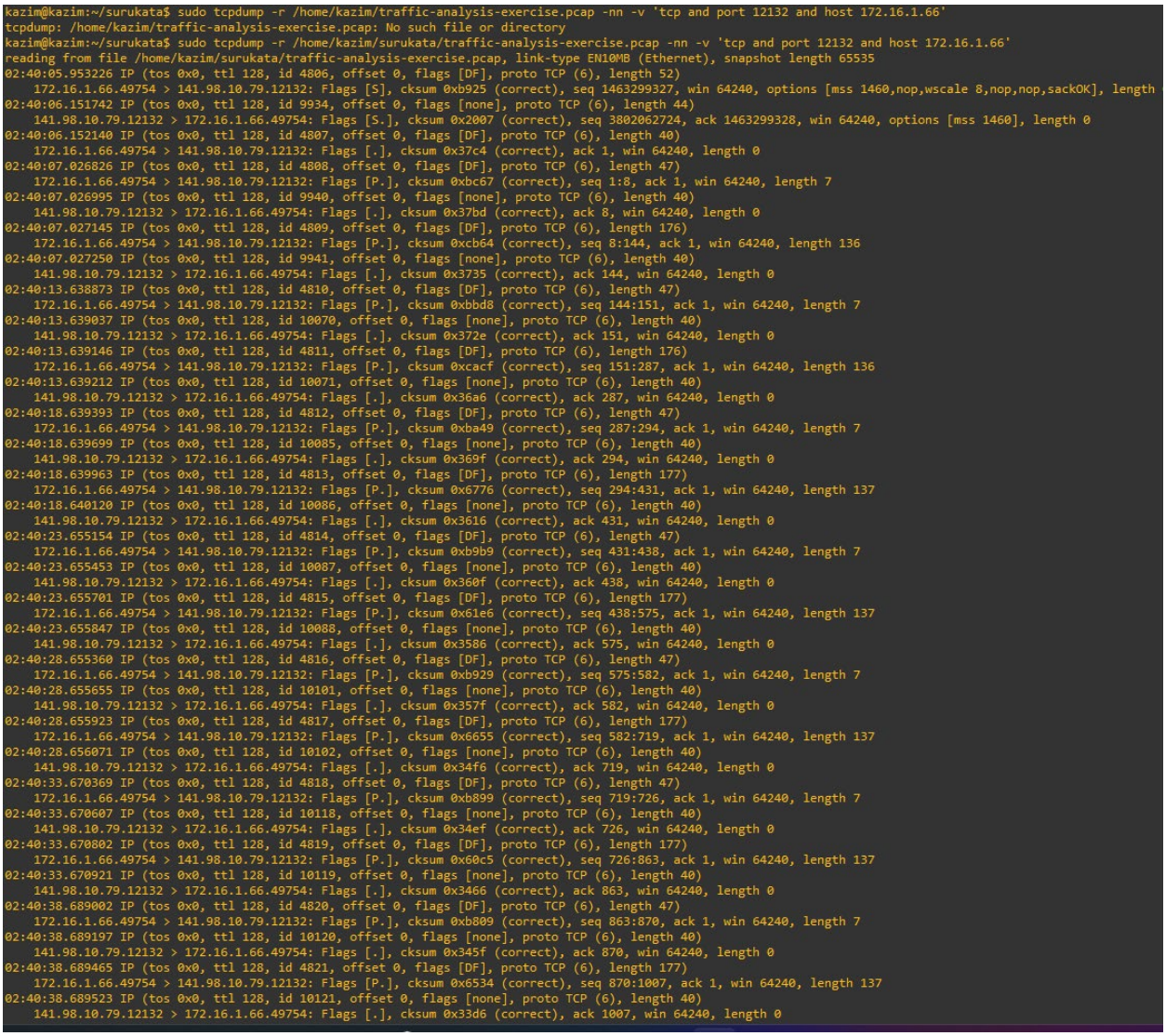


Figure (5) Show the data flow between the infected system, internal resources, and external C&C server, highlighting where the malicious activity is taking place.



```
kazim@kazim:~/surukata$ sudo tcpdump -r /home/kazim/traffic-analysis-exercise.pcap -nn -v 'tcp and port 12132 and host 172.16.1.66'
tcpdump: /home/kazim/traffic-analysis-exercise.pcap: No such file or directory
kazim@kazim:~/surukata$ sudo tcpdump -r /home/kazim/surukata/traffic-analysis-exercise.pcap -nn -v 'tcp and port 12132 and host 172.16.1.66'
reading from file /home/kazim/surukata/traffic-analysis-exercise.pcap, link-type EN10MB (Ethernet), snapshot length 65535
02:40:05.953226 IP (tos 0x0, ttl 128, id 4806, offset 0, flags [DF], proto TCP (6), length 52)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [S], cksum 0xb925 (correct), seq 1463299327, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length
02:40:06.151742 IP (tos 0x0, ttl 128, id 9934, offset 0, flags [none], proto TCP (6), length 44)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [S.], cksum 0x2007 (correct), seq 3802062724, ack 1463299328, win 64240, options [mss 1460], length 0
02:40:06.152140 IP (tos 0x0, ttl 128, id 4807, offset 0, flags [DF], proto TCP (6), length 40)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [.], cksum 0x37c4 (correct), ack 1, win 64240, length 0
02:40:07.026826 IP (tos 0x0, ttl 128, id 4808, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xbc67 (correct), seq 1:8, ack 1, win 64240, length 7
02:40:07.026995 IP (tos 0x0, ttl 128, id 9940, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x37bd (correct), ack 8, win 64240, length 0
02:40:07.027145 IP (tos 0x0, ttl 128, id 4809, offset 0, flags [DF], proto TCP (6), length 176)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xcb64 (correct), seq 8:144, ack 1, win 64240, length 136
02:40:07.027250 IP (tos 0x0, ttl 128, id 9941, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x3735 (correct), ack 144, win 64240, length 0
02:40:13.638873 IP (tos 0x0, ttl 128, id 4810, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xbbd8 (correct), seq 144:151, ack 1, win 64240, length 7
02:40:13.639037 IP (tos 0x0, ttl 128, id 10070, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x372e (correct), ack 151, win 64240, length 0
02:40:13.639146 IP (tos 0x0, ttl 128, id 4811, offset 0, flags [DF], proto TCP (6), length 176)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xcacf (correct), seq 151:287, ack 1, win 64240, length 136
02:40:13.639212 IP (tos 0x0, ttl 128, id 10071, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x36a6 (correct), ack 287, win 64240, length 0
02:40:18.639393 IP (tos 0x0, ttl 128, id 4812, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xba49 (correct), seq 287:294, ack 1, win 64240, length 7
02:40:18.639699 IP (tos 0x0, ttl 128, id 10085, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x369f (correct), ack 294, win 64240, length 0
02:40:18.639963 IP (tos 0x0, ttl 128, id 4813, offset 0, flags [DF], proto TCP (6), length 177)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0x6776 (correct), seq 294:431, ack 1, win 64240, length 137
02:40:18.640120 IP (tos 0x0, ttl 128, id 10086, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x3616 (correct), ack 431, win 64240, length 0
02:40:23.655154 IP (tos 0x0, ttl 128, id 4814, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xb9b9 (correct), seq 431:438, ack 1, win 64240, length 7
02:40:23.655453 IP (tos 0x0, ttl 128, id 10087, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x360f (correct), ack 438, win 64240, length 0
02:40:23.655701 IP (tos 0x0, ttl 128, id 4815, offset 0, flags [DF], proto TCP (6), length 177)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0x61e6 (correct), seq 438:575, ack 1, win 64240, length 137
02:40:23.655847 IP (tos 0x0, ttl 128, id 10088, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x3586 (correct), ack 575, win 64240, length 0
02:40:28.655360 IP (tos 0x0, ttl 128, id 4816, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xb929 (correct), seq 575:582, ack 1, win 64240, length 7
02:40:28.655655 IP (tos 0x0, ttl 128, id 10101, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x357f (correct), ack 582, win 64240, length 0
02:40:28.655923 IP (tos 0x0, ttl 128, id 4817, offset 0, flags [DF], proto TCP (6), length 177)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0x6655 (correct), seq 582:719, ack 1, win 64240, length 137
02:40:28.656071 IP (tos 0x0, ttl 128, id 10102, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x34f6 (correct), ack 719, win 64240, length 0
02:40:33.670369 IP (tos 0x0, ttl 128, id 4818, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xb899 (correct), seq 719:726, ack 1, win 64240, length 7
02:40:33.670607 IP (tos 0x0, ttl 128, id 10118, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x34ef (correct), ack 726, win 64240, length 0
02:40:33.670802 IP (tos 0x0, ttl 128, id 4819, offset 0, flags [DF], proto TCP (6), length 177)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0x60c5 (correct), seq 726:863, ack 1, win 64240, length 137
02:40:33.670921 IP (tos 0x0, ttl 128, id 10119, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x3466 (correct), ack 863, win 64240, length 0
02:40:38.689002 IP (tos 0x0, ttl 128, id 4820, offset 0, flags [DF], proto TCP (6), length 47)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0xb809 (correct), seq 863:870, ack 1, win 64240, length 7
02:40:38.689197 IP (tos 0x0, ttl 128, id 10120, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x345f (correct), ack 870, win 64240, length 0
02:40:38.689465 IP (tos 0x0, ttl 128, id 4821, offset 0, flags [DF], proto TCP (6), length 177)
    172.16.1.66.49754 > 141.98.10.79.12132: Flags [P.], cksum 0x6534 (correct), seq 870:1007, ack 1, win 64240, length 137
02:40:38.689523 IP (tos 0x0, ttl 128, id 10121, offset 0, flags [none], proto TCP (6), length 40)
    141.98.10.79.12132 > 172.16.1.66.49754: Flags [.], cksum 0x33d6 (correct), ack 1007, win 64240, length 0
```

Figure (6) **Packet Capture Overview**: A snippet of the captured packets showing **TCP port 12132 communication** between the infected system and the C&C server.

Conclusion and Remediation

- **Conclusion**: The analysis confirms that 172.16.1.66 (DESKTOP-SKBR25F) is compromised with **STRRAT** malware. It is actively attempting to communicate with an external C&C server, 141.98.10.79. Immediate action is required to isolate the system and block the external IP address to prevent further communication.
- **Recommended Actions**:

    1. **Disconnect** the infected system from the network.
    2. **Block IP address** 141.98.10.79 at the perimeter firewall.
    3. **Conduct a full malware scan** and remove any identified threats.
    4. **Change all credentials** used by the affected system, especially if any **Netlogon** attributes were compromised.
    5. **Review LDAP logs** for any additional signs of lateral movement.