DDoS Incident Response

Room 40 - Cyber “40oz”
Rubin, Brayan, and Jose

Monitoring Sources

1. CIC-IDS2017 (Network IDS PCAP)

- **Purpose**: Captured raw packet data to analyze traffic patterns and identify DDoS-related anomalies.
- **Analysis Capabilities**:
  - Detected spikes in traffic volume from single or distributed sources.
  - Identified abnormal packet characteristics such as SYN floods, UDP floods, or malformed packets.
- **Relevance to DDoS**:
  - Provided granular details of malicious traffic for forensic analysis.
  - Flagged high volumes of requests targeting a single server port or service.

2. Splunk (Log Aggregation and Analysis Platform)

- **Purpose**: Aggregated logs from multiple infrastructure components to visualize attack patterns.
- **Analysis Capabilities**:
  - Correlated traffic data from firewalls, load balancers, and servers to confirm attack origin.
  - Enabled historical comparisons to identify deviations from baseline traffic volumes.
  - Generated automated alerts for traffic surges exceeding pre-configured thresholds.
- **Relevance to DDoS**:
  - Pinpointed originating IP addresses and suspected botnets.
  - Mapped attack vectors, such as layer 7 (HTTP floods) or layer 3/4 (SYN floods, UDP floods).

Impact Analysis and Triage

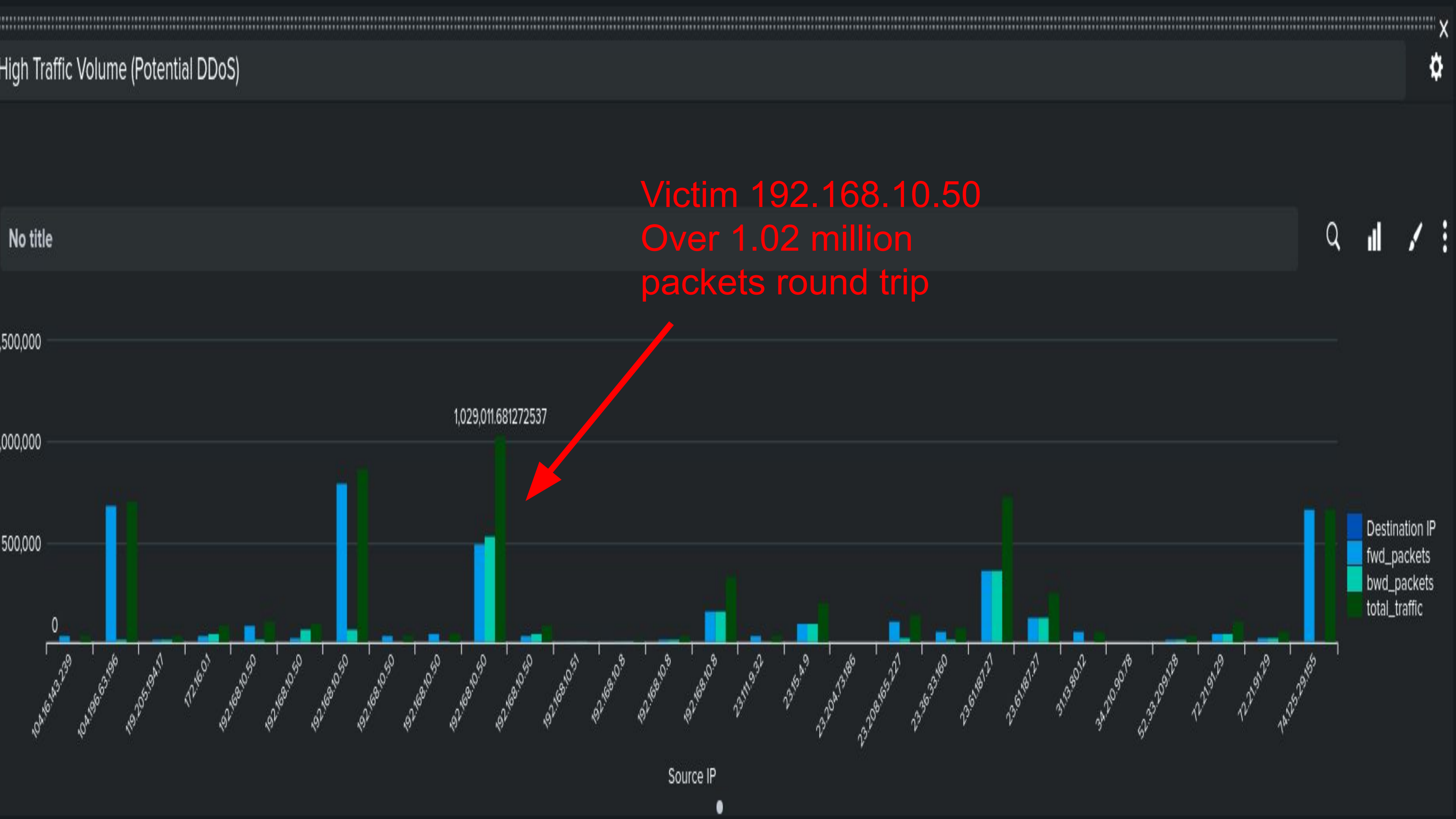
Impact Analysis

- **Severity Determination**:
  - The attack involved a **DDoS LOIT** (Low Orbit Ion Cannon), a widely used tool for generating high-volume flood attacks.
  - **Target**: The victim identified as `192.168.10.50`, which experienced over **1.02 million packets round trip**, indicating significant service disruption risk.
  - **Severity**: Assessed as **critical** due to the overwhelming traffic volume and potential collateral damage to interconnected systems.
- **Affected Systems**:
  - **Primary Victim**: `192.168.10.50`.
  - **Potential Impact**: Additional systems within the network may have experienced degraded performance due to shared resources or routing load.
- **Prioritization**:
  - **Immediate Actions**:
    - Implement traffic rate limiting on the primary victim.
    - Analyze and block traffic from high-traffic sources such as `192.168.10.50` and `172.16.0.1`.

Impact Analysis and Triage cont’d

Triage Process

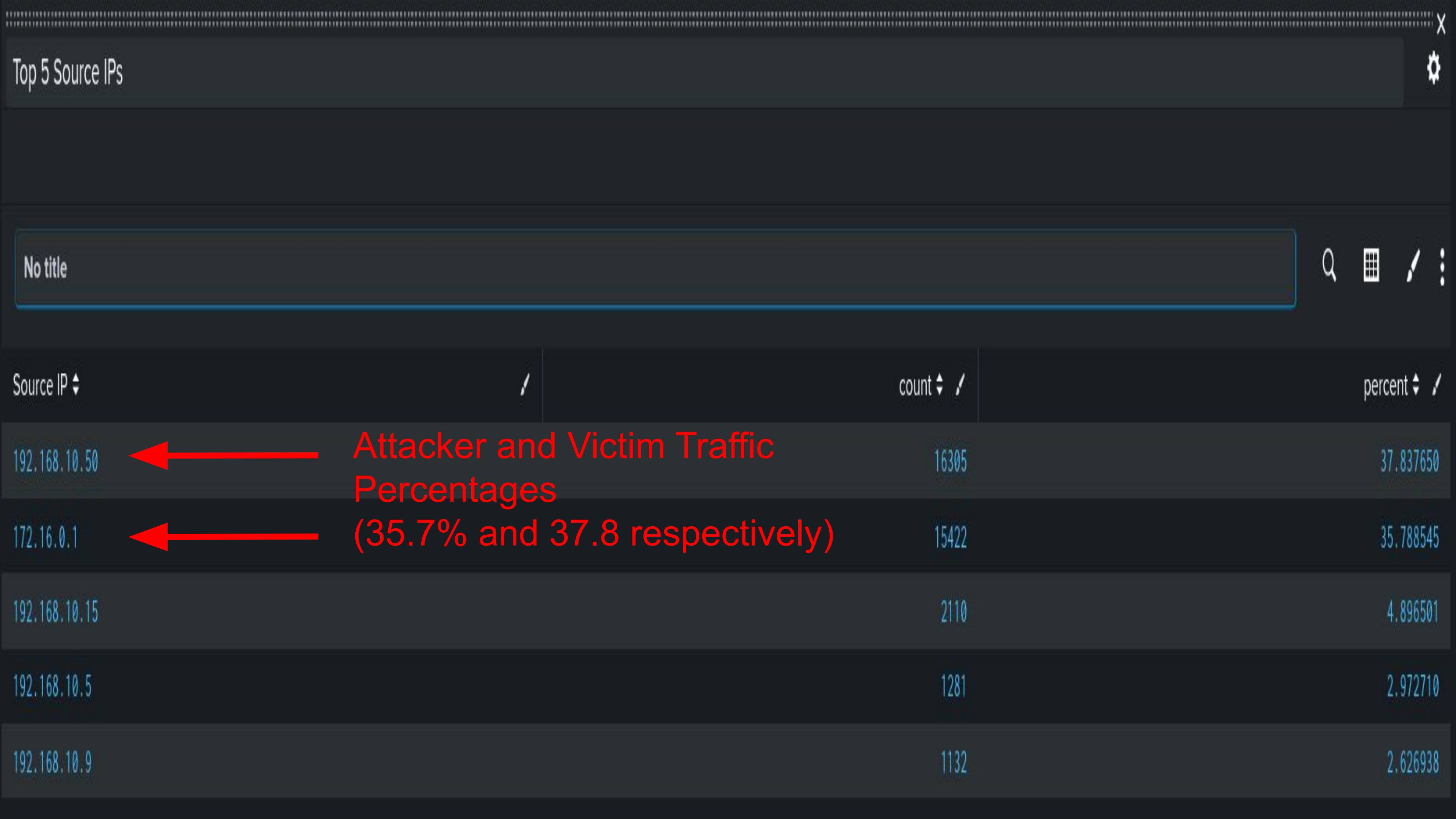
- **Scope Identification**:
  - **Key Attacker IPs**:
    - `192.168.10.50`: Experienced bursts of **37.8% of total traffic**.
    - `172.16.0.1`: Contributed **35.7% of total traffic**, indicating its role in the attack chain.
  - **Victim IP**: `192.168.10.50` experienced the majority of the inbound attack.
  - **Attack Timeframe**: Confirmed during **15:56 – 16:16**.
- **Additional Systems Affected**:
  - Investigate firewall and local traffic logs to verify spillover impact on adjacent systems or critical services.
- **Recommendations**:
  - Enhance detection thresholds for abnormal traffic patterns, especially focusing on top traffic generators (`192.168.10.50`, `172.16.0.1`).
  - Conduct post-mitigation analysis to ensure residual effects are addressed.



High Traffic Volume (Potential DDoS)

No title

Victim 192.168.10.50
Over 1.02 million
packets round trip



Top 5 Source IPs

No title

Source IP	count	percent
192.168.10.50	16305	37.837650
172.16.0.1	15422	35.788545
192.168.10.15	2110	4.896501
192.168.10.5	1281	2.972710
192.168.10.9	1132	2.626938

Attacker and Victim Traffic Percentages
(35.7% and 37.8 respectively)

Identified Assets and Critical Services Under Attack

DNS Servers (Port 53):

The most targeted port in terms of total traffic volume.

Web Servers (Port 80):

Port 80 was also heavily targeted, showing significant **anomalous traffic spikes**, as detected by Splunk.

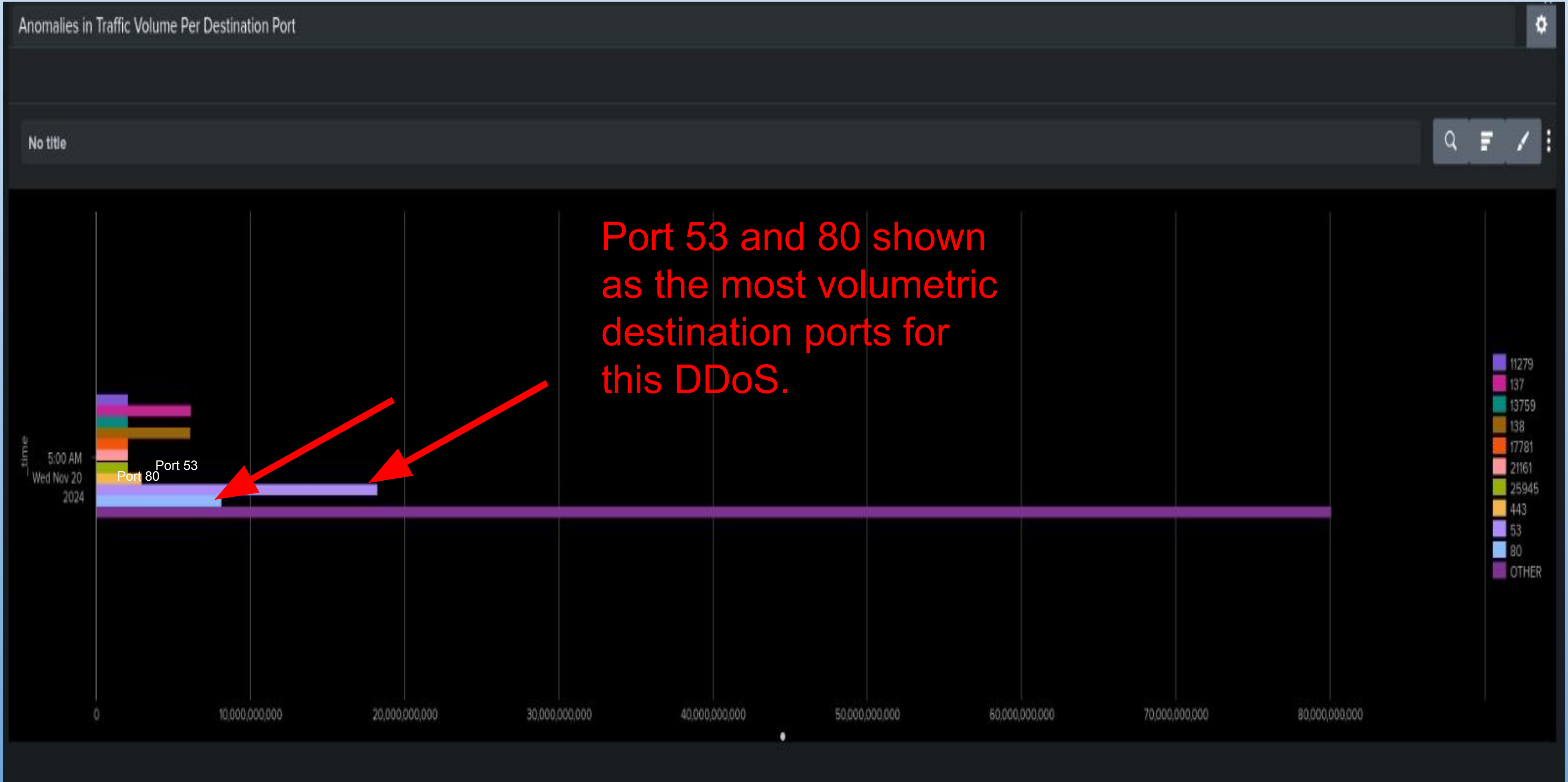
HTTPS Services (Port 443):

Port 443 (HTTPS) is targeted to overwhelm SSL/TLS encrypted connections, affecting secure services, showing a multi-vector attack strategy.

Splunk and Anomaly Detection:

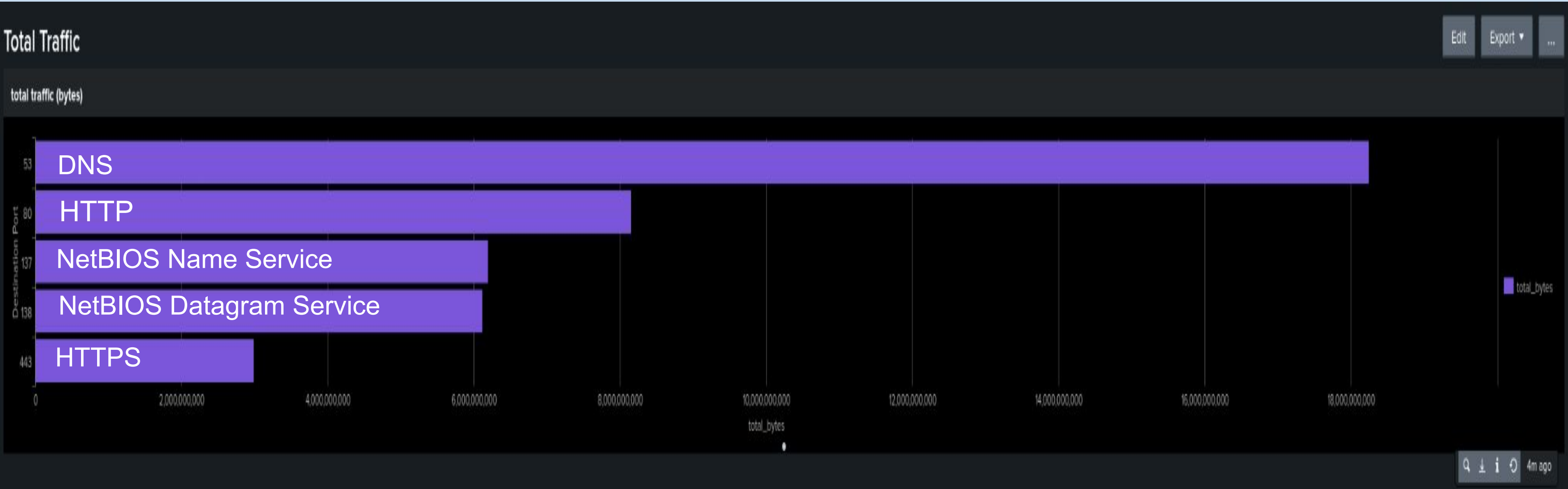
Splunk enabled real-time tracking of traffic anomalies and SYN flags, identifying ports targeted in the DDoS attack, helping prioritize the response efforts for affected services.

Anomalies in Traffic Volume



Port 53 and 80 shown as the most volumetric destination ports for this DDoS.

Total Traffic Per Ports



Threat Intelligence

Splunk and Threat Intelligence:

- **Splunk** helped **gather and analyze threat intelligence** in real time.
- Correlated **traffic anomalies** with **known attack signatures** to identify attack timing and targeted ports.
- **SYN flood**, **HTTP flood** patterns were key indicators of a **LOIT attack**.
- **Anomaly detection** in **Splunk** helped detect **traffic surges**, correlating with DDoS tactics.

Indicators of Compromise (IOCs):

- **SYN flood packets** and **high traffic to critical ports** (Port 80, Port 53) were clear **IOCs**.

Tactics, Techniques, and Procedures (TTPs):

- The attack used common DDoS tactics, like **SYN floods** and **HTTP floods**.
- Focused on **Port 80 (HTTP)** and **Port 53 (DNS)**, consistent with known **LOIT attack patterns**.
- Allowed us to **predict attack behavior**, **identify attack vectors**, and **prepare defenses**.

Recommended Remediation

1. Patching Systems

- Regularly update and patch software, firmware, and applications to fix known vulnerabilities.
- Use automated patch management tools like WSUS, Ansible, or SCCM to ensure consistency.

2. Firewall Rules

- Implement rate-limiting rules to restrict excessive traffic from a single IP or source.
- Restrict access to critical ports like 80 (HTTP) and 443 (HTTPS) to trusted IPs when feasible.

3. Proactive Monitoring

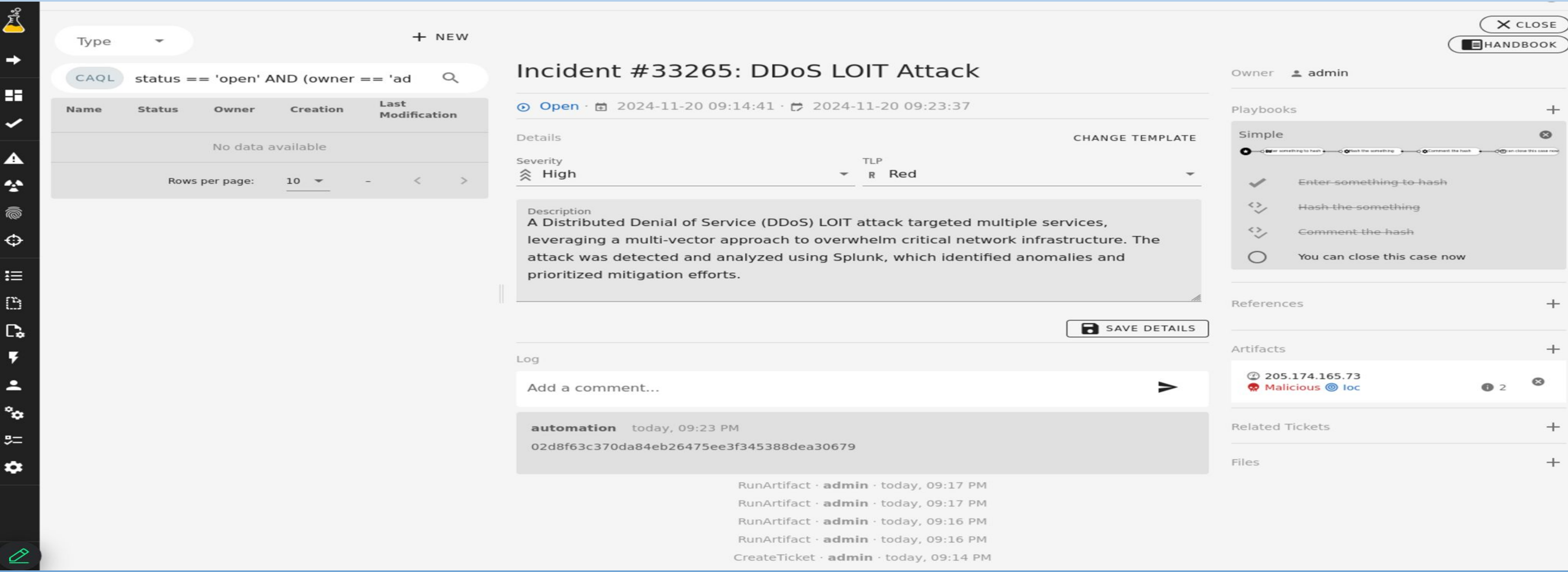
- Use Splunk to continuously monitor traffic and generate real-time alerts for anomalies.

4. Incident Response Playbook

- Develop and document a detailed response playbook based on lessons learned from this incident.

Case Management System

We used Catalyst to setup case management and Incident Response logging



CAQL status == 'open' AND (owner == 'ad

Name	Status	Owner	Creation	Last Modification
No data available				

Rows per page: 10 -

Incident #33265: DDoS LOIT Attack

Open · 2024-11-20 09:14:41 · 2024-11-20 09:23:37

Details

Severity: High

TLP: R Red

Description
A Distributed Denial of Service (DDoS) LOIT attack targeted multiple services, leveraging a multi-vector approach to overwhelm critical network infrastructure. The attack was detected and analyzed using Splunk, which identified anomalies and prioritized mitigation efforts.

Log

Add a comment...

```
automation   today, 09:23 PM
02d8f63c370da84eb26475ee3f345388dea30679

RunArtifact · admin · today, 09:17 PM
RunArtifact · admin · today, 09:17 PM
RunArtifact · admin · today, 09:16 PM
RunArtifact · admin · today, 09:16 PM
CreateTicket · admin · today, 09:14 PM
```

Owner: admin

Playbooks

Simple

- ✓ ~~Enter something to hash~~
- ~~Hash the something~~
- ~~Comment the hash~~
- ○ You can close this case now

References

Artifacts

205.174.165.73
Malicious Ioc 2

Related Tickets

Files

THANK YOU !