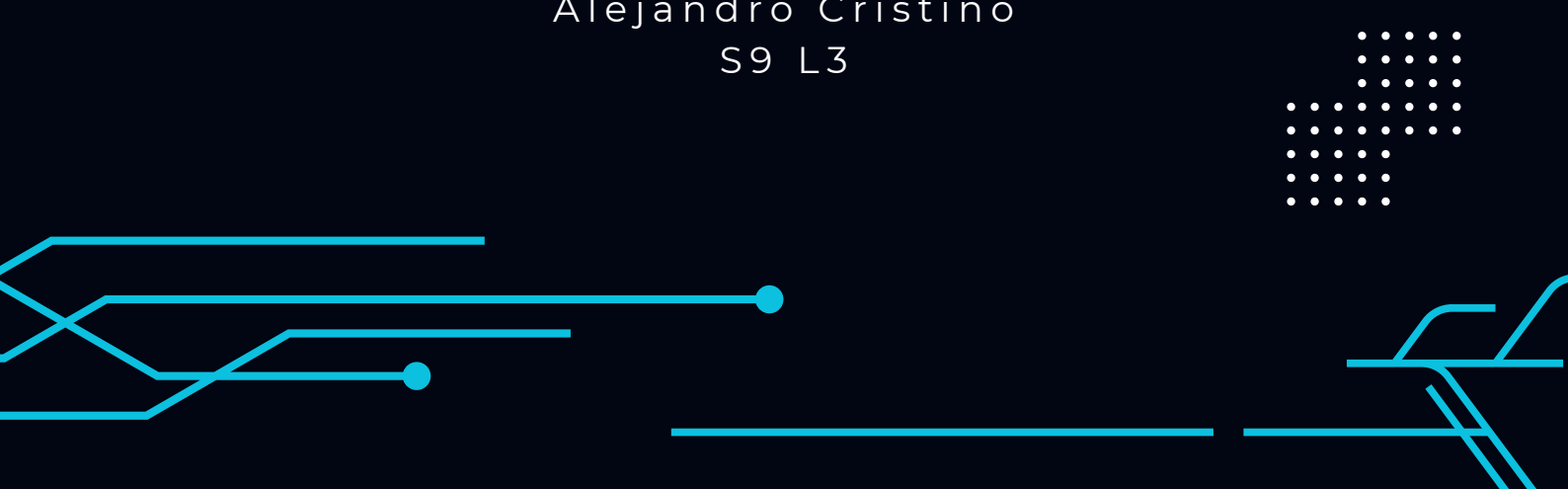




# ***REPORT***

## *THREAT INTELLIGENCE & IOC*

Alejandro Cristino  
S9 L3



## 1. Identificare eventuali IOC

Indicazioni dalla cattura di rete:

### 1. Porte sospette e protocolli utilizzati:

- Ci sono molte richieste TCP con porte di destinazione come 33876 e 33943, che potrebbero essere associate a comportamenti sospetti, come il tentativo di brute force o la scansione di porte.
- Molti pacchetti con flag RST, SYN e ACK indicano possibili tentativi di connessione non autorizzata o scansioni di rete.
- La presenza di numerosi pacchetti TCP con SYN e RST può indicare tentativi di connessione falliti o una potenziale scansione delle porte.

### 2. IP sorgenti e destinazioni:

- L'IP 192.168.200.150 appare frequentemente come destinazione, suggerendo che potrebbe essere l'obiettivo principale dell'attacco.
- L'IP 192.168.200.100 e l'IP 192.168.200.255 sono anche ripetutamente coinvolti, il che può suggerire che siano sorgenti o intermediari.

## 2. Ipotesi sui potenziali vettori di attacco

- Scansione delle porte: L'elevato numero di pacchetti SYN e RST suggerisce una scansione delle porte per identificare servizi aperti o vulnerabili su 192.168.200.150.
- Tentativi di accesso non autorizzato: L'uso di pacchetti SYN per diverse porte può indicare tentativi di brute force o di sfruttare vulnerabilità note.
- Spoofing o Attacco Man-in-the-Middle (MitM): La presenza di numerosi pacchetti con flag TCP non standard può anche indicare un tentativo di spoofing o un attacco MitM.

## 3. Azioni per ridurre gli impatti dell'attacco

- Isolare l'host compromesso: Bloccare temporaneamente l'accesso dell'IP 192.168.200.150 dalla rete per prevenire ulteriori danni.
- Implementare firewall e IDS: Configurare un firewall per bloccare le richieste sospette e un sistema di rilevamento delle intrusioni (IDS) per monitorare attività insolite.
- Aggiornare i sistemi e i software: Assicurarsi che tutti i sistemi e software siano aggiornati con le ultime patch di sicurezza per prevenire lo sfruttamento di vulnerabilità note.
- Monitorare i log e le connessioni di rete: Analizzare i log di sistema e di rete per identificare ulteriori segni di compromissione e stabilire una linea temporale degli eventi.