Threat Intelligence

Guardando attentamente le immagini si possono notare vari indicatori di compromissioni. Ad esempio la quantità di pacchetti TCP con flag RST possono indicare attività di scansione delle porte o tentativi di interruzione delle connessioni attive, può essere un port scanning aggressivo o un tentativo di attacco DoS. Un numero elevato di pacchetti SYN potrebbe indicare un tentativo di SYN Flooding, un tipo di attacco DoS in cui un attaccante tenta di saturare le risorse di rete con richieste di connessione incomplete. Si può notare anche la presenza di pacchetti ARP che possono essere correlati a possibili attacchi ARP spoofing o Man-in-the-Middle per intercettare il traffico. In base agli IOC identificati, possiamo fare alcune ipotesi sui potenziali vettori di attacco e le tecniche utilizzate:

1. *Port scanning e Reconnaissance*
    - Indicatore: Traffico TCP con molti pacchetti RST
    - Vettore di attacco: Port scanning
    - Ipotesi: L'attaccante potrebbe essere alla ricerca di porte aperte sui sistemi della rete per individuare servizi vulnerabili da sfruttare in un attacco successivo.
    - Obiettivo: Raccogliere informazioni sulla rete per capire quali porte e servizi sono esposti, magari preparando un attacco mirato.
    - Soluzione: Per prevenire il port scanning consigliamo di configurare il firewall per bloccare o limitare le richieste da IP sospetti o sconosciuti e implementare tecniche di port knocking per nascondere le porte aperte. Mentre per rilevare scansioni di porte aperte è possibile utilizzare strumenti di **Intrusion Detection System** come **Snort** o **Suricata**.
2. *SYN Flooding*
    - Indicatore: Alto numero di pacchetti SYN senza ACK corrispondenti
    - Vettore di attacco: SYN Flood
    - Ipotesi: L'attaccante sta cercando di sovraccaricare le risorse di rete del target inviando un numero eccessivo di richieste di connessione TCP incomplete.
    - Obiettivo: Rendere il sistema bersaglio non disponibile per i servizi legittimi.
    - Soluzioni: Per prevenire attacchi Dos si consiglia di limitre il numero di connessoni simultanee per IP, abilitare SYN Cookies per proteggere le risorse del server getsendo richieste di handshake non completate e configurare un firewall o sistemi di prevenzioni DDoS come AWS Shield.
3. *Session Hijacking o Spoofing*
    - Indicatore: Pacchetti TCP con **Seq=1, Ack=1** e presenza di traffico ARP.

- Vettore di attacco: Session Hijacking o TCP Spoofing.
- Ipotesi: Un attaccante potrebbe tentare di prendere il controllo di una sessione già stabilita falsificando pacchetti TCP o utilizzando ARP Spoofing per dirottare il traffico verso la propria macchina.
- Obiettivo: Intercettare o alterare la comunicazione per rubare dati sensibili o eseguire comandi maliziosi.

4. *Man-in_the-Middle / ARP spoofing*
    - Indicatore: Elevato numero di pacchetti ARP anomali.
    - Vettore di attacco: ARP Spoofing.
    - Ipotesi: Un attaccante potrebbe tentare di posizionarsi come intermediario tra due dispositivi nella rete, manipolando le tabelle ARP per intercettare o alterare il traffico.
    - Obiettivo: Catturare credenziali, intercettare dati, o iniettare contenuti malevoli nelle comunicazioni.
    - Soluzioni: Configurare manualmente le tabelle ARP per dispositivi critici, usare switch di rete gestiti con funzionalità di protezione ARP e isolare le reti sensibili da quelle pubbliche. Mentre per monitorare modifiche sospette alle tabelle ARP si possono usare strumenti come **ARPWatch**.