**Report di Analisi: Threat Intelligence & IOC**

**Introduzione**

Questo report presenta l'analisi di una cattura di rete effettuata tramite **Wireshark** per identificare eventuali **Indicatori di Compromissione (IOC)** e formulare ipotesi su potenziali vettori di attacco. L'obiettivo è valutare possibili minacce presenti nella rete analizzata e fornire raccomandazioni su come mitigare i rischi futuri.

**1. Panoramica dei Dati**

La cattura di rete include traffico TCP, ARP e HTTP/HTTPS tra dispositivi nella rete locale **192.168.200.x**. Sono stati analizzati pacchetti provenienti da vari host, con particolare attenzione a:

* **PCSSystemtec\_39:7d:...**: un host rilevato tramite richieste ARP.
* Comunicazioni tra **192.168.200.100**, **192.168.200.150**, e altri dispositivi della rete.

**2. Indicatori di Compromissione (IOC) Identificati**

**a. Attività ARP Anomala**

* Durante l'analisi, è stato rilevato traffico ARP ripetuto, con richieste provenienti da **PCSSystemtec\_39:7d:...**, che chiedeva risoluzioni ARP per gli indirizzi **192.168.200.100** e **192.168.200.150**.
* **Possibile Minaccia**: Questo tipo di traffico potrebbe indicare una normale attività di scoperta di rete o, potenzialmente, un tentativo di **ARP Spoofing**. Il numero elevato di richieste ARP potrebbe essere segnale di un attacco in corso, volto a intercettare il traffico tra dispositivi.

**b. Tentativi di Connessione TCP Falliti (RST, ACK)**

* Sono stati identificati diversi pacchetti **TCP** con flag **RST, ACK**, che indicano che il dispositivo di destinazione (principalmente **192.168.200.100**) ha respinto tentativi di connessione da **192.168.200.150**.
* **Possibile Minaccia**: Questi pacchetti potrebbero indicare tentativi di connessione non autorizzati o falliti, potenzialmente parte di una scansione di rete o di un attacco brute-force. Se questi tentativi si ripetono su porte diverse, si potrebbe ipotizzare che l'attaccante stia cercando di individuare vulnerabilità nella rete.

**c. Traffico HTTP/HTTPS**

* È stato rilevato traffico su **porta 80 (HTTP)** e **porta 443 (HTTPS)** tra dispositivi locali. Tuttavia, non sono stati identificati immediatamente indirizzi IP esterni sospetti.
* **Possibile Minaccia**: Il traffico su porte standard come **80** e **443** potrebbe indicare normale attività di navigazione web, ma richiede ulteriori approfondimenti se si trovano connessioni verso IP sconosciuti o server esterni che potrebbero essere malevoli. Queste connessioni potrebbero essere tentativi di comunicazione di malware.

**d. Uso di Porte Elevate**

* Sono stati osservati pacchetti TCP provenienti da porte elevate come **52358**, **33878** e **46138**.
* **Possibile Minaccia**: L'uso di porte elevate non standard potrebbe essere un tentativo di bypassare sistemi di sicurezza o firewall. Questi pacchetti dovrebbero essere monitorati per ulteriori verifiche su possibili attività malevole.

**3. Ipotesi sui Vettori di Attacco**

**a. ARP Spoofing**

Le ripetute richieste ARP potrebbero indicare un tentativo di **ARP Spoofing**, in cui un attaccante cerca di intercettare il traffico tra dispositivi fingendo di essere un altro host. Questo tipo di attacco può permettere all'attaccante di ottenere dati sensibili o reindirizzare il traffico.

**b. Scansioni di rete e tentativi brute-force**

I tentativi di connessione ripetuti falliti con pacchetti **RST, ACK** potrebbero essere indicativi di una scansione di rete in corso, in cui un attaccante cerca di mappare i dispositivi attivi e individuare porte aperte per sfruttare vulnerabilità. Se confermato, potrebbe anche essere un tentativo di brute-force su servizi esposti.

**c. Comunicazioni malevole (HTTP/HTTPS)**

Il traffico su porte **HTTP** e **HTTPS** può indicare tentativi di comunicazione verso server esterni. Se indirizzato a server sospetti, questo potrebbe essere un vettore di esfiltrazione dati o un canale per la comunicazione di malware.

**4. Azioni Raccomandate**

1. **Monitoraggio ARP**: Implementare tecniche di mitigazione contro ARP spoofing, come l'uso di **ARP statici** sui dispositivi critici o l'implementazione di strumenti di rilevamento delle intrusioni (IDS) per monitorare e bloccare tali attività.
2. **Blocco di IP Sospetti**: Configurare il firewall per bloccare indirizzi IP che tentano ripetutamente di stabilire connessioni non autorizzate o che utilizzano porte elevate non standard.
3. **Audit delle Connessioni HTTPS**: Se sono stati identificati server sconosciuti o sospetti nelle connessioni HTTPS, effettuare un audit per verificare se qualche dispositivo sta comunicando con server malevoli o con domini sconosciuti.
4. **Protezione contro brute-force**: Implementare limitazioni di tentativi di login o servizi esposti (ad esempio, utilizzando protezioni contro brute-force su RDP, SSH, ecc.) e chiudere le porte inutilizzate.
5. **Utilizzo di IDS/IPS**: Implementare sistemi di rilevamento/prevenzione delle intrusioni per monitorare traffico sospetto e generare alert in caso di attività malevole.

**Conclusioni**

L'analisi della cattura di rete ha evidenziato alcuni potenziali Indicatori di Compromissione che richiedono un monitoraggio attento e l'implementazione di misure di sicurezza per prevenire attacchi futuri. Sebbene non siano stati rilevati attacchi conclamati, l'attività anomala nelle richieste ARP e nei tentativi di connessione respinti potrebbe indicare che è in corso una scansione di rete o tentativi di compromissione.