Threat Intelligence & IOC

1. Identificazione e analisi degli IOC (Indicator of Compromise)

Ho aperto e analizzato il file `Cattura_U3_W1_L5.pcapng` tramite **Wireshark** l'analisi evidenzia tentativi di connessione da una macchina compromessa verso una macchina vulnerabile, osservando il traffico tra due host interni alla rete:

- **Sorgente**: `192.168.200.100`
- **Destinazione**: `192.168.200.150`

I pacchetti sono tutti basati sul **protocollo TCP**, ma con un comportamento anomalo:

Comportamenti sospetti rilevati:

- Sono presenti **molte connessioni fallite** con pacchetti di tipo `SYN-ACK`, che indicano che la macchina destinataria sta **rifiutando** le richieste.
- Le connessioni sono dirette verso **porte insolite**, come:

  4443 (simile alla 443, ma spesso usata da malware per nascondersi)

  63686, **52358**, **56120** → porte molto alte, non utilizzate da servizi comuni

- Alcune connessioni avvengono anche sulla **porta 80 (HTTP)**, ma non sembra esserci traffico HTTP effettivo. È possibile che la porta venga usata per nascondere altro tipo di comunicazione.

  Questo tipo di traffico è tipico di una reverse shell, cioè un attaccante che tenta di prendere controllo del sistema remoto attraverso una porta personalizzata.

Inoltre, **la frequenza dei pacchetti** e la varietà delle porte usate suggeriscono un tentativo automatico di connessione, tipico di un **malware attivo** in esecuzione.

2. Ipotesi sui vettori di attacco utilizzati

Una volta identificati gli IOC, possiamo formulare un'ipotesi su **come è avvenuta la compromissione**.

Vettori di attacco possibili:

- Il traffico parte dalla macchina `192.168.200.100`, quindi **è quella il probabile punto di "infezione"**.
- Il tipo di comunicazione fa pensare a un **file eseguibile malevolo (.exe)** scaricato o eseguito su quella macchina. Questo file può aver avviato:

    Una **reverse shell**, che cerca di connettersi a `192.168.200.150` (possibile macchina dell'attaccante nella LAN).

    Un **client malware** che tenta di comunicare con un server C2 per ricevere comandi.

Questo scenario si verifica spesso quando un utente:

- Apre un allegato e-mail infetto
- Scarica un programma da un sito compromesso

Il fatto che le connessioni siano tutte **interne alla LAN** potrebbe indicare un **movimento laterale**, cioè un malware che, una volta installato, cerca di propagarsi all'interno della rete aziendale.

3. Azioni consigliate per ridurre l'impatto dell'attacco attuale e prevenire futuri attacchi

Una volta individuata la macchina compromessa, è fondamentale agire subito per **contenere il danno**, ma anche per **prevenire futuri attacchi simili**.

Contromisure immediate (incident response):

1. **Isolare il dispositivo `192.168.200.100` dalla rete**: in questo modo si interrompe ogni possibile comunicazione con l'attaccante o con altri dispositivi.

2. **Bloccare le porte sospette a livello di firewall**:

   4443, 63686, 52358, 56120 → porte alte non utilizzate da servizi legittimi.

3. **Analizzare il sistema sospetto**:

   Eseguire una scansione con antivirus/antimalware aggiornati.

   Controllare se sono presenti eseguibili anomali o processi attivi non riconosciuti.

4. **Raccolta dei log e delle prove** per un'analisi forense e per eventuale report all'azienda o agli enti preposti.

Azioni preventive:

1. **Implementare un sistema IDS/IPS** (Intrusion Detection/Prevention System), per rilevare comportamenti sospetti in tempo reale.

2. **Segmentare la rete** in VLAN per isolare server, client e dispositivi critici.

3. **Aggiornare regolarmente antivirus e software** su tutte le macchine della rete.

4. **Formazione agli utenti finali**: insegnare a riconoscere e-mail sospette, siti non sicuri e file infetti.

5. **Attivare logging centralizzato e alerting** su tentativi di accesso su porte non comuni.