S9/L5

Report di Analisi Forense di Rete: Identificazione e Risposta a Minacce Avanzate

Data: 30 Maggio 2025

Autore: Francesco Fontana

Riferimento: Indagine su Attività Sospette nella Rete Interna

1. Premessa dell'Indagine

Un'approfondita analisi di una sessione di cattura di rete, eseguita con l'ausilio di Wireshark, ha portato alla luce chiari Indicatori di Compromissione (IOC) che suggeriscono un'attività malevola in corso all'interno della rete locale. L'attenzione investigativa si è concentrata in particolare sul flusso di traffico anomalo tra l'host con indirizzo IP 192.168.200.100 e la destinazione 192.168.200.150.

2. Rilevamento degli Indicatori di Compromissione (IOC)

L'esame meticoloso del traffico ha permesso di identificare diversi IOC cruciali, che delineano le fasi di un potenziale attacco:

- **Scansione di Rete Estensiva:** È stata rilevata una scansione di rete di vasta portata, con un volume superiore a 2000 pacchetti dedicati alla scansione delle porte. Questo elevato numero di tentativi indica una fase attiva di ricognizione all'interno della rete interna, finalizzata a mappare l'infrastruttura e individuare bersagli vulnerabili.
- **Tentativi di Connessione su Porta TCP 445 (SMB):** Sono stati osservati numerosi tentativi di stabilire connessioni sulla porta TCP 445, comunemente associata al protocollo Server Message Block (SMB). Tali attività suggeriscono potenziali tentativi di accesso non autorizzato o di sfruttamento di vulnerabilità note su condivisioni di rete, spesso riconducibili a minacce come EternalBlue.
- **Traffico SMB con Protocollo Browser:** La presenza di traffico SMB che impiega il protocollo Browser è un segnale inequivocabile di un'enumerazione attiva delle risorse di rete e dei dispositivi disponibili, indicando una fase di raccolta informazioni dettagliata da parte dell'aggressore.
- **Connessione su Porta TCP 33042 (Anomala):** È stata identificata una connessione su una porta TCP non standard, la 33042. Questa porta è stata utilizzata per lo scambio di dati binari sospetti, la cui natura non è riconducibile a protocolli di comunicazione legittimi o comunemente impiegati.

3. Analisi Approfondita del Flusso di Dati sulla Porta 33042

Un'indagine più approfondita ha rivelato la presenza di quattro pacchetti TCP sulla porta 33042, caratterizzati da un effettivo scambio di dati payload. Questo dettaglio è di fondamentale importanza, poiché conferma che la connessione è stata stabilita con successo e non si è trattato di un mero tentativo di handshake.

L'esame del contenuto esadecimale e ASCII di questi pacchetti ha mostrato sequenze di dati binari che non corrispondono a protocolli standard come HTTP, SSH o SMB. La combinazione di questa porta non convenzionale e il tipo di traffico rilevato indica con elevata probabilità l'esistenza di un canale di comando e controllo (C2), una reverse shell o un meccanismo di esfiltrazione dati, tutti elementi distintivi di un'infezione malware attiva.

4. Scenario di Attacco Ipotizzato

Sulla base degli indicatori rilevati e dell'analisi del traffico, si formula l'ipotesi che l'host 192.168.200.100 sia stato compromesso e sia attivamente coinvolto in attività malevole. Le fasi dell'attacco sembrano seguire un percorso ben definito:

- **Fase di Ricognizione Attiva:** L'host compromesso ha eseguito scansioni sistematiche per identificare altri host e porte aperte all'interno della rete.
- **Fase di Enumerazione e Tentativi di Sfruttamento:** Sono stati condotti tentativi di enumerazione e di sfruttamento di vulnerabilità SMB su altri host della rete, con particolare attenzione verso 192.168.200.150.
- **Fase di Stabilizzazione del Canale Nascosto:** È stato instaurato un canale di comunicazione occulto sulla porta non standard 33042, presumibilmente per il controllo remoto dell'host compromesso o per l'esfiltrazione di dati sensibili.

5. Misure Correttive Raccomandate

Per mitigare l'attacco in corso e prevenire ulteriori compromissioni, si raccomandano le seguenti azioni immediate e strategiche a lungo termine:

- **Isolamento Immediato dell'Host:** L'host 192.168.200.100 deve essere immediatamente disconnesso dalla rete per impedire la propagazione dell'attacco o ulteriori movimenti laterali.
- **Verifica Approfondita dell'Host 192.168.200.150:** È indispensabile condurre una verifica completa dell'host 192.168.200.150 per rilevare eventuali compromissioni o attività anomale che potrebbero essere state indotte dall'attacco.
- **Analisi Forense Completa degli Endpoint:** Eseguire un'analisi forense approfondita su tutti gli endpoint coinvolti, includendo scansioni antivirus/EDR (Endpoint Detection and Response) e un controllo meticoloso dei processi attivi e delle configurazioni.
- **Revisione e Rafforzamento delle Policy di Sicurezza:** Le policy di sicurezza esistenti devono essere riviste e rafforzate, con un'attenzione particolare alla segmentazione della rete e al blocco delle porte non necessarie (ad esempio, SMB tra host utente, porte alte non documentate).
- **Implementazione di Sistemi di Monitoraggio e Allerta:** È fondamentale implementare o potenziare sistemi di monitoraggio e allerta come IDS/IPS (Intrusion Detection/Prevention

Systems) e SIEM (Security Information and Event Management) per intercettare attività sospette in tempo reale e generare risposte rapide.

- **Applicazione Tempestiva di Patch e Aggiornamenti:** Assicurare l'applicazione immediata di patch e aggiornamenti critici su tutti i dispositivi di rete e i sistemi operativi per correggere vulnerabilità note e ridurre la superficie di attacco.

6. Considerazioni Finali

L'analisi della cattura di rete ha permesso di identificare un attacco interno multi-fase, caratterizzato da una fase iniziale di scansione, seguita da enumerazione e tentativi di sfruttamento di vulnerabilità SMB, e culminato nell'instaurazione di un canale di comunicazione remoto su una porta non standard.

Intervenire prontamente con le misure consigliate è di cruciale importanza per contenere i danni attuali e prevenire la replicazione di attacchi simili in futuro, salvaguardando così la sicurezza e l'integrità dell'infrastruttura di rete.