Phantom srl

2024 REPORT

PREPARED BY

PIGNATELLO GIUSEPPE
ALESSIO D'OTTAVIO
LUCA IANNONE

PRESENTED BY

PHANTOM SRL

Table of Contents

CONTENTS

INTRODUCTION

Quest'oggi andremo a spiegare cosa sono e come si presentano gli IOC e cosa si intende quando parliamo di Threat Intelligence.
Successivamente andremo a vedere un esempio pratico per chiarire le idee a riguardo, vediamo la traccia:
Analizzare la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di attacchi in corso
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

SPIEGAZIONE INDICATOR OF COMPROMISE

Quando si verifica un incidente di web security, gli indicatori di compromissione (IoC) costituiscono la prova del data breach.
Queste tracce digitali rivelano non soltanto che è avvenuto l'incidente, ma spesso permettono anche di scoprire quali strumenti sono stati usati per sferrare l'attacco e da chi.
Gli indicatori di compromissione possono anche essere utilizzati per determinare in quale grado l'incidente informatico abbia colpito l'organizzazione, e per mettere in sicurezza la rete da possibili attacchi futuri.
Gli indicatori vengono tipicamente raccolti da appositi software, come gli antivirus e gli anti malware, ma anche nuovi strumenti basati sull'intelligenza artificiale, vengono utilizzati sempre più spesso per aggregare e organizzare gli indicatori durante le fasi di incident response.

SPIEGAZIONE THREAT INTELLIGENCE

La threat intelligence - detta anche 'CTI' (cyber threat intelligence) o 'threat intel' - consiste in dati contenenti informazioni dettagliate sulle minacce alla sicurezza informatica che prendono di mira un'organizzazione. La TI aiuta i team di sicurezza a essere più proattivi, consentendo loro di intraprendere azioni efficaci e basate sui dati per prevenire gli attacchi informatici prima che si verifichino. Può anche aiutare un'organizzazione a rilevare e rispondere meglio agli attacchi in corso. Gli analisti della sicurezza creano la threat intelligence raccogliendo informazioni non elaborate sulle minacce e correlate alla sicurezza da molteplici fonti, procedendo quindi a correlare e analizzare i dati per scoprire tendenze, schermi e relazioni che forniscono una comprensione approfondita delle minacce effettive o potenziali. Le informazioni che ne derivano sono Specifiche per l'organizzazione, focalizzate non su informazioni generiche (ad es. elenchi di ceppi di malware comuni) ma sulle specifiche vulnerabilità nella superficie di attacco dell'organizzazione, sugli attacchi che consentono e sugli asset che espongono.

SPIEGAZIONE E RISOLUZIONE ESERCITAZIONE

Dai pacchetti catturati, possiamo dedurre diversi aspetti del traffico di rete tra gli indirizzi IP 192.168.200.100 e 192.168.200.150 utilizzando il protocollo TCP. Ecco alcune osservazioni in base ai dati forniti:

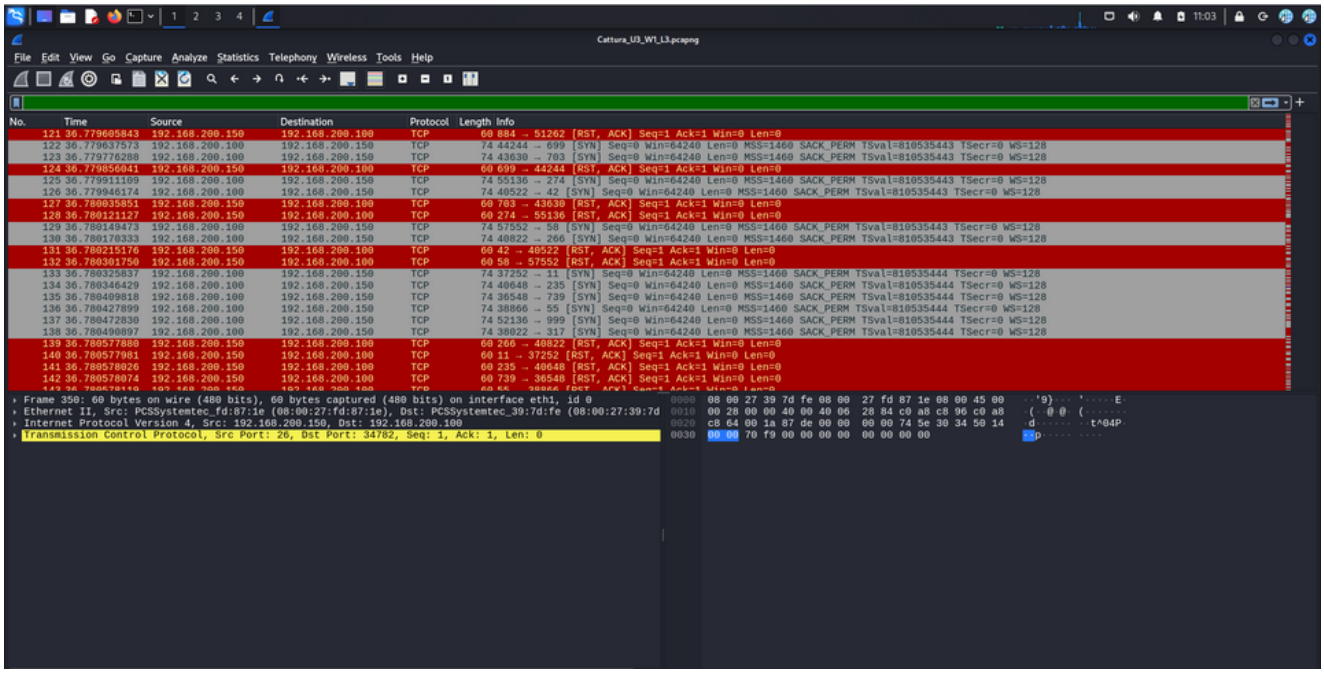
Connessioni TCP iniziate: Ci sono diverse connessioni TCP iniziate dal mittente (192.168.200.100) verso il destinatario (192.168.200.150). Queste connessioni sono identificate dai pacchetti con il flag [SYN] (synchronization) nel campo "Info".

Reset delle connessioni: Dopo l'invio dei pacchetti di sincronizzazione [SYN], ci sono risposte di reset delle connessioni (flag [RST]) dai destinatari (192.168.200.150), indicando che le connessioni non sono state stabilite correttamente o sono state interrotte in modo anomalo.

Dimensioni dei pacchetti: I pacchetti hanno varie dimensioni (campo "Length"), indicando una diversità nel carico di dati trasmessi tra i due host.

Altre informazioni TCP: I pacchetti includono informazioni come la finestra di congestione (campo "Win"), il valore MSS (Maximum Segment Size), i timestamp, che sono tutti elementi tipici dei pacchetti TCP e possono essere utilizzati per ottimizzare le prestazioni della connessione.

Deduciamo quindi che l'attaccante (avente indirizzo ip 192.168.200.100) sta effettuando una scansione delle porte (information gathering attivo) sulla macchina vittima (avente indirizzo ip 192.168.200.150).



REMEDIATION ACTIONS

Per mitigare o prevenire tentativi di scansione o altri tipi di attività sospette sulla rete, si possono adottare diverse azioni di rimedio. Ecco alcune misure da considerare:

Configurare correttamente il firewall: Assicurarsi che il firewall sia configurato correttamente per bloccare il traffico non autorizzato o sospetto. Limitare l'accesso solo ai servizi e alle porte necessarie e bloccare l'accesso alle porte non utilizzate o comunemente associate a tentativi di scansione, ed in questo caso bloccare l'IP della macchina conducente attività anomale**.**

Impostare filtri sul router: Utilizzare filtri di pacchetti o altri meccanismi di controllo del traffico sul router per limitare l'accesso alla rete e bloccare il traffico sospetto in ingresso e in uscita.

Monitoraggio del traffico di rete: Utilizzare strumenti di monitoraggio del traffico di rete per individuare e rispondere prontamente a comportamenti anomali o sospetti. Si possono utilizzare strumenti come Wireshark o IDS/IPS (Intrusion Detection/Prevention System) per rilevare e bloccare tentativi di scansione e altri attacchi.

Aggiornare e patchare regolarmente: È importante aggiornare i sistemi operativi, le applicazioni e gli apparati di rete con gli ultimi aggiornamenti e patch di sicurezza per correggere eventuali vulnerabilità note che potrebbero essere sfruttate dagli attaccanti.

Configurare regole di accesso: Utilizzare regole di accesso ACL (Access Control List) per consentire solo il traffico autorizzato da e verso determinati indirizzi IP, porte o protocolli specifici.

Implementare la gestione delle minacce: Utilizzare soluzioni di gestione delle minacce per identificare e mitigare attivamente le minacce alla sicurezza della rete, come intrusioni, malware o tentativi di scansione.

Educazione degli utenti: Assicurarsi che gli utenti della rete siano consapevoli dei rischi legati alla sicurezza informatica e impartisci formazione sulla sicurezza delle informazioni per promuovere comportamenti sicuri e consapevoli.

Analisi dei log: Monitorare regolarmente i log di sicurezza dei dispositivi di rete e dei sistemi per individuare attività sospette e rispondere prontamente a eventuali anomalie.

Implementando queste misure, è possibile contribuire a proteggere la rete da tentativi di scansione e altre minacce alla sicurezza informatica.

Consigliamo l'utilizzo costante dei seguenti tool per monitorare e analizzare il traffico di rete e recuperare informazioni preziose al fine di prevenire ogni tipologia di attacco informatico.

PHANTOM s.r.l
IMPOSSIBLE IS
OUR TARGET

PHANTOM
SRL
SINCE 2024

GRAZIE PER L'ATTENZIONE

PIGNATELLO GIUSEPPE

IANNONE LUCA

D'OTTAVIO ALESSIO