



THREAT INTELLIGENCE & IOC

INTRODUZIONE



Durante l'analisi di una cattura di rete effettuata con Wireshark, sono stati individuati potenziali Indicatori di Compromissione (IOC) che suggeriscono attività sospette e potenzialmente malevole. L'obiettivo di questa analisi è identificare e valutare i vettori di attacco, determinare la loro natura e proporre contromisure adeguate per mitigare sia l'attacco in corso che futuri attacchi di natura simile.

ANALISI DEGLI INDICATORI DI COMPROMISSIONE

Connessioni TCP Anomale

Osservazione: L'IP 192.168.200.100 (sospettato come attaccante) ha inviato pacchetti SYN a numerose porte di destinazione sul dispositivo 192.168.200.150 (presunta vittima), tra cui:

- Porta 80 (HTTP)
- Porta 443 (HTTPS)
- Porta 135 (RPC)
- Porta 993 (IMAP)
- Porta 21 (FTP)

In ciascun caso, la sequenza di handshake TCP è incompleta, risultando in un pattern:

- SYN → SYN/ACK → RST/ACK.

Interpretazione:

- Scansione delle Porte: L'attaccante effettua una scansione SYN TCP su varie porte del bersaglio per riconoscere le porte attive o no.
- SYN Flood: Anche se non c'è saturazione evidente, il traffico potrebbe essere parte di un attacco DoS a basso volume per testare la resistenza della macchina.
- Tecniche di evasione: Il reset immediato della connessione potrebbe essere un tentativo di evitare il rilevamento da parte di strumenti di monitoraggio.

Questo pattern suggerisce una scansione Nmap rapida (-T4), con l'esecuzione di handshake TCP (SYN, SYN-ACK, ACK), il che indica l'uso di una scansione completa delle connessioni (-sT).

Impatto Potenziale:

Un attaccante che identifica porte vulnerabili può sfruttarle per ottenere accesso non autorizzato, eseguire exploit o persino compromettere completamente il sistema.

FILTRO TCP

tcp						
	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535438 WS=64
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
29	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
30	36.775386694	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53062 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
32	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.775619454	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
35	36.775796938	192.168.200.150	192.168.200.100	TCP	74	22 → 55656 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
36	36.775797004	192.168.200.150	192.168.200.100	TCP	74	80 → 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535439 WS=64
37	36.775803786	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
39	36.775861964	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
41	36.776005853	192.168.200.100	192.168.200.150	TCP	66	53062 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=4294952466
42	36.776179338	192.168.200.100	192.168.200.150	TCP	74	50684 → 199 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
43	36.776233880	192.168.200.100	192.168.200.150	TCP	74	54220 → 995 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535439 TSecr=0 WS=128
44	36.776330610	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
45	36.776385694	192.168.200.100	192.168.200.150	TCP	74	33042 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128
46	36.776402500	192.168.200.100	192.168.200.150	TCP	74	49814 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535440 TSecr=0 WS=128

ANOMALIE NEI PACCHETTI ARP

L'analisi dei pacchetti ARP tra gli indirizzi IP 192.168.200.100 e 192.168.200.150 ha evidenziato ripetute richieste ARP tra i due dispositivi.

Interpretazione: ARP Spoofing / MITM (Man-In-The-Middle): La presenza di risposte ARP inconsistenti suggerisce la possibilità di un attacco di ARP Spoofing, che potrebbe essere finalizzato a un attacco Man-In-The-Middle (MITM). Un elemento sospetto che suggerisce un possibile attacco MITM è che la prima comunicazione rilevata sia una richiesta SYN sulla porta 80, piuttosto che una normale richiesta ARP. Inoltre, la successiva richiesta ARP suggerisce che i due dispositivi non si siano mai precedentemente comunicati. Tuttavia, senza ulteriori dati, non è possibile trarre una conclusione definitiva riguardo a un attacco MITM in corso.

```
8 28.761629461 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP
9 28.761644619 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP
10 28.774852257 PCSSystemtec_39:7d:... PCSSystemtec_fd:87:... ARP
11 28.775230099 PCSSystemtec_fd:87:... PCSSystemtec_39:7d:... ARP
```

IPOTESI SUI VETTORI DI ATTACCO

Scenari Possibili:

1. Attacco Interno: L'attaccante si trova nella stessa rete della vittima e sta sfruttando l'accesso diretto per lanciare attacchi (es. scansione delle porte, ARP Spoofing).
2. Esplorazione di Servizi Vulnerabili: La scansione delle porte potrebbe preludere all'uso di exploit su servizi noti, come per esempio vulnerabilità RPC o FTP.

```
60 Who has 192.168.200.100? Tell 192.168.200.150
42 192.168.200.100 is at 08:00:27:39:7d:fe
42 Who has 192.168.200.150? Tell 192.168.200.100
60 192.168.200.150 is at 08:00:27:fd:87:1e
```

RACCOMANDAZIONI PER LA MITIGAZIONE



01

Monitoraggio e Blocco del Traffico Sospetto:

- Configurare il firewall per limitare il numero di connessioni SYN incomplete per IP sorgente.
- Impostare regole che bloccano o limitano l'accesso alle porte non necessarie.

02

Rafforzamento della Rete:

- Isolare i dispositivi critici della rete aziendale in subnet dedicate.
- Utilizzare Virtual LAN (VLAN) per limitare la comunicazione tra segmenti non correlati.

03

Interventi ARP:

- Configurare tabelle ARP statiche sui dispositivi più importanti, associando manualmente IP e MAC.
- Implementare Dynamic ARP Inspection (DAI) sugli switch per prevenire risposte ARP fasulle.

06

STRATEGIE A MEDIO-LUNGO TERMINE

01

Implementazione di IDS/IPS (Intrusion Detection/Prevention Systems):

- Utilizzare strumenti come Snort, Suricata o Zeek per rilevare tentativi di scansione delle porte, ARP Spoofing e altre attività sospette in tempo reale.

02

Educazione e Formazione:

- Formare il personale IT e il team SOC per riconoscere comportamenti di rete anomali.
- Sensibilizzare gli utenti aziendali sui rischi degli attacchi interni e su come segnalare eventuali anomalie.

03

Audit della Sicurezza:

- Effettuare una valutazione periodica della rete per identificare vulnerabilità, come servizi non necessari esposti a internet o configurazioni errate

04

Segmentazione della Rete:

- Limitare l'accesso tra dispositivi non correlati attraverso l'uso di ACL (Access Control Lists) e policy di segmentazione.



CONCLUSIONE



L'analisi preliminare suggerisce che la rete è stata bersaglio di attività malevoli, tra cui una scansione delle porte. L'origine dell'attacco sembra essere interna, il che enfatizza l'importanza di monitorare attentamente le reti aziendali.

THANK YOU