

S9L5

Luca Calvigioni

THREAT INTELLIGENCE E IOC

Per Threat Intelligence si intende la raccolta, l'analisi e la condivisione di informazioni su minacce attuali e potenziali alla sicurezza informatica. Queste informazioni includono dettagli sui cyber attacchi, sulle vulnerabilità dei sistemi, sulle tattiche degli attaccanti e sugli indicatori di compromissione IoC. Gli IoC sono evidenze o eventi di un attacco in corso, oppure già avvenuto, elenchiamone alcuni:

- Indirizzi IP sospetti
- Hash di file
- Url o domini malevoli
- Pacchetti syn senza completamento della stretta di mano a 3 vie
- Processi anomali ecc

Oggi andremo ad analizzare una cattura di rete effettuata con Wireshark e risponderemo ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC.
- Fare delle ipotesi sui potenziali vettori di attacco utilizzati.
- Consigliare un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.200.150	192.168.200.255	ICMP	60	Host Announcement: 192.168.200.255
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53966 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=0 WS=128
3	23.764237700	192.168.200.100	192.168.200.150	TCP	74	53976 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53966 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810522427 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33976 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	60	53966 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=429495246
7	23.764858991	192.168.200.150	192.168.200.100	TCP	60	33976 → 443 [ACK] Seq=1 Ack=1 Win=0 Len=0
8	28.761629401	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	60	Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	42	192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852571	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	42	Who has 192.168.200.100? Tell 192.168.200.150
11	28.775230999	PcsCompu_39:7d:fe	PcsCompu_39:7d:fe	ARP	60	192.168.200.150 is at 08:00:27:39:7d:fe
12	36.774134445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
13	36.774211115	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33976 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535438 TSecr=0 WS=128
16	36.774409027	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 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=1 TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41102 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
19	36.774685905	192.168.200.100	192.168.200.150	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=429495246 TSecr=810535437 WS=64
20	36.774685952	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=1 TSval=429495246 TSecr=810535437 WS=64
21	36.774696000	192.168.200.100	192.168.200.150	TCP	60	443 → 33976 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774696000	192.168.200.100	192.168.200.150	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774695737	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774695776	192.168.200.150	192.168.200.100	TCP	60	993 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	36.774708464	192.168.200.100	192.168.200.150	TCP	60	41102 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=429495246
26	36.774711072	192.168.200.100	192.168.200.150	TCP	60	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=429495246
27	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	36.775141104	192.168.200.150	192.168.200.100	TCP	60	41102 → 21 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	36.775140448	192.168.200.100	192.168.200.150	TCP	60	41102 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=429495246
30	36.775337800	192.168.200.100	192.168.200.150	TCP	74	59174 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535438 TSecr=0 WS=128
31	36.775389594	192.168.200.100	192.168.200.150	TCP	74	55656 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
32	36.775524204	192.168.200.100	192.168.200.150	TCP	74	53962 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
33	36.775589806	192.168.200.150	192.168.200.100	TCP	60	113 → 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	36.775619454	192.168.200.150	192.168.200.100	TCP	60	41304 → 23 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	36.775652497	192.168.200.100	192.168.200.150	TCP	60	56120 → 111 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	36.775709338	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=1 TSval=810535439 TSecr=810535439 WS=64
37	36.775719004	192.168.200.100	192.168.200.150	TCP	74	80 → 53962 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=429495246 TSecr=810535439 WS=64
38	36.775803786	192.168.200.100	192.168.200.150	TCP	60	55656 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495246
39	36.775813232	192.168.200.100	192.168.200.150	TCP	60	53962 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495246
40	36.775823078	192.168.200.100	192.168.200.150	TCP	60	41102 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495246
41	36.775975876	192.168.200.100	192.168.200.150	TCP	60	55656 → 22 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

No.	Time	Source	Destination	Protocol	Length	Info
40	36.775975876	192.168.200.100	192.168.200.150	TCP	60	55056 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495246
41	36.776058553	192.168.200.100	192.168.200.150	TCP	60	53962 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535439 TSecr=429495246
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=1 TSval=810535439 TSecr=0 WS=128
43	36.776233886	192.168.200.100	192.168.200.150	TCP	74	54220 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535439 TSecr=0 WS=128
44	36.776306100	192.168.200.100	192.168.200.150	TCP	74	34648 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
45	36.776359694	192.168.200.100	192.168.200.150	TCP	74	33842 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
46	36.776407500	192.168.200.100	192.168.200.150	TCP	74	49814 → 290 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 → 50684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	993 → 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49	36.776471201	192.168.200.100	192.168.200.150	TCP	74	46990 → 133 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
50	36.776496366	192.168.200.100	192.168.200.150	TCP	74	33206 → 143 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
51	36.776512221	192.168.200.100	192.168.200.150	TCP	74	60632 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
52	36.776560606	192.168.200.100	192.168.200.150	TCP	74	49054 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
53	36.776671271	192.168.200.100	192.168.200.150	TCP	74	37282 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
54	36.776720715	192.168.200.100	192.168.200.150	TCP	74	54898 → 500 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	77 → 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
56	36.776842423	192.168.200.150	192.168.200.100	TCP	74	51534 → 407 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
57	36.776904828	192.168.200.150	192.168.200.100	TCP	74	445 → 33842 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=429495246 TSecr=810535440 WS=64
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	25 → 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59	36.776904951	192.168.200.150	192.168.200.100	TCP	74	433 → 49990 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=429495246 TSecr=810535440 WS=64
60	36.776905004	192.168.200.150	192.168.200.100	TCP	60	143 → 33206 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61	36.776905043	192.168.200.150	192.168.200.100	TCP	74	25 → 60632 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=429495246 TSecr=810535440 WS=64
62	36.776905052	192.168.200.150	192.168.200.100	TCP	60	110 → 49054 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63	36.776905123	192.168.200.150	192.168.200.100	TCP	74	53 → 37282 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=810535440 WS=64
64	36.776905102	192.168.200.150	192.168.200.100	TCP	60	500 → 54898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776917772	192.168.200.100	192.168.200.150	TCP	60	33842 → 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=429495246
66	36.776941020	192.168.200.100	192.168.200.150	TCP	60	46990 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=429495246
67	36.776962320	192.168.200.100	192.168.200.150	TCP	60	60632 → 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=429495246
68	36.776983870	192.168.200.100	192.168.200.150	TCP	60	37282 → 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535440 TSecr=429495246
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	407 → 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70	36.777143914	192.168.200.100	192.168.200.150	TCP	74	56990 → 707 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
71	36.777186821	192.168.200.100	192.168.200.150	TCP	74	35638 → 436 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535440 TSecr=0 WS=128
72	36.777303991	192.168.200.100	192.168.200.150	TCP	74	34120 → 90 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
73	36.777337934	192.168.200.100	192.168.200.150	TCP	74	49708 → 78 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
74	36.777436632	192.168.200.150	192.168.200.100	TCP	60	707 → 56990 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777439741	192.168.200.150	192.168.200.100	TCP	60	436 → 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76	36.777473918	192.168.200.100	192.168.200.150	TCP	74	36138 → 588 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
77	36.777522494	192.168.200.100	192.168.200.150	TCP	74	52428 → 902 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
78	36.777623030	192.168.200.150	192.168.200.100	TCP	60	33976 → 24120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49708 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Identificazione IOC

- L'Indirizzo IP del presunto attaccante è privato, ciò vuol dire che l'attaccante si trova nella nostra stessa rete locale (LAN)
- Ripetuti pacchetti SYN provenienti dall'indirizzo IP 192.168.200.100 senza concludere la stretta di mano a 3 vie tipica del protocollo TCP (SYN, SYN/ACK, ACK) quindi al posto di ACK l'attaccante invierà un RST per interrompere la connessione, questo può essere un segno di un port scanning.
- Risposta RST da parte del server 192.168.200.150 sta ad indicare una sorta di protezione e quindi interrompe la connessione o semplicemente potrebbe essere che la porta è chiusa.
- Traffico elevato di pacchetti SYN (SYN FLOOD) provenienti dalla stessa sorgente in modo ripetitivo può essere un chiaro segno di attacco DoS.

Ipotesi

In base agli IOC identificati possiamo fare le seguenti ipotesi sui vettori di attacco:

- SYN FLOOD (Denial of Service): L'attaccante invia pacchetti SYN per aprire connessioni TCP senza completare il processo di handshake. Ciò può esaurire le risorse del server, rendendolo indisponibile per altri utenti a causa del numero elevato di richieste da gestire. Questo prende il nome di attacco DoS
- PORT SCANNING: È probabile che l'attaccante stia utilizzando uno strumento di scanning come ad esempio NMAP per verificare la presenza di servizi attivi sulle porte aperte e di conseguenza prepararsi per ulteriori exploit.
Ipotizzando un comando nmap che l'attaccante può aver lanciato

nmap -sT -p- -Pn 192.168.200.150

-sT permette di completare la connessione e subito dopo chiuderla con RST,ACK

-p- scansiona tutte e 65535 le porte logiche.

-Pn omette la fase di invio del ping, per bypassare firewall o comunque eludere sistemi di rilevamento di intrusione.

Consigli e misure preventive

Per ridurre l'impatto dell'attacco attuale e prevenire futuri attacchi simili, è necessario adottare un approccio che combini misure immediate, configurazioni preventive e strategie a lungo termine.

- Bloccare o comunque limitare l'indirizzo IP sospetto impostando una regola del firewall, questo impedirà ulteriori tentativi di connessione dall'attaccante
- Analizzare in tempo reale il traffico di rete per individuare eventuali attività sospette non provenienti dall'IP bloccato. Questo permette di identificare altri potenziali attaccanti o variazioni dell'attacco, questo vale anche per prevenire futuri attacchi.
- Se sono presenti porte aperte che non ospitano servizi attivi, chiuderle immediatamente. Questo riduce la superficie di attacco e limita l'efficacia di scansioni multi-porta.
- Utilizzare sistemi di rilevamento e prevenzione delle intrusioni come IDS/IPS per identificare e bloccare attacchi DoS automaticamente.
- Imporre limiti sulle connessioni TCP, ovvero regole che limitino il numero di connessioni incomplete per ogni IP sorgente, ad esempio un SYN FLOOD protection.
- Aggiornamento costante di dispositivi e software per chiudere vulnerabilità note.
- Ultimo ma non per importanza è il sensibilizzare gli utenti ad adottare buone pratiche di sicurezza informatica.

Conclusioni

Tirando le Somme si tratta di una Scansione Nmap perchè viene generato un traffico limitato e sequenziale con l'obiettivo è raccogliere informazioni sulle porte aperte e non sovraccaricare il sistema, al contrario di un attacco Dos che punta ad esaurire la capacità del server con l'invio di migliaia o milioni di pacchetti.

Per concludere possiamo dire che adottare misure immediate per contenere l'attacco corrente è cruciale, ma prevenire attacchi futuri richiede una combinazione di configurazioni preventive, monitoraggio continuo e buone pratiche di sicurezza. Il rafforzamento della rete e dei server riduce la superficie di attacco e migliora la prevenzione da attacchi sempre più sofisticati.