

Nell'esercizio di oggi dobbiamo individuare gli indicatori di compromissione (IOC) in un file di wireshark. Gli indicatori di compromissione sono delle prove, osservabili all'interno di una rete o sistema, che possono indicare un'intrusione. Indicatori tipici possono essere firme antivirali, connessioni TCP/UDP elevate o provenienti dallo stesso mittente e diretti su porte diverse, indirizzi IP o URL sospetti, ecc.

Nel file si possono identificare connessioni TCP multiple:

12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41384	→ 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	36.774495627	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	→ 41384 [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=810535437 WS=64
21	36.774685656	192.168.200.150	192.168.200.100	TCP	60	413	→ 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	36.774709464	192.168.200.100	192.168.200.150	TCP	66	41384	→ 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	36.775174848	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

Come possiamo osservare nella figura sopra ci sono molte richieste TCP che partono dallo stesso mittente e vanno ognuna su una porta diversa. Stessa cosa per l'immagine sotto:

133	36.780325837	192.168.200.100	192.168.200.150	TCP	74	37252	→ 11 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
134	36.780346429	192.168.200.100	192.168.200.150	TCP	74	40648	→ 235 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
135	36.780409818	192.168.200.100	192.168.200.150	TCP	74	30548	→ 739 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
136	36.780427899	192.168.200.100	192.168.200.150	TCP	74	38866	→ 55 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
137	36.780472830	192.168.200.100	192.168.200.150	TCP	74	52136	→ 999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
138	36.780490897	192.168.200.100	192.168.200.150	TCP	74	38022	→ 317 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535444 TSecr=0 WS=128
139	36.780577880	192.168.200.150	192.168.200.100	TCP	60	266	→ 40822 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
140	36.780577981	192.168.200.150	192.168.200.100	TCP	60	11	→ 37252 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
141	36.780578026	192.168.200.150	192.168.200.100	TCP	60	235	→ 40648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
142	36.780578074	192.168.200.150	192.168.200.100	TCP	60	739	→ 30548 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
143	36.780578119	192.168.200.150	192.168.200.100	TCP	60	55	→ 38866 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
144	36.780578158	192.168.200.150	192.168.200.100	TCP	60	999	→ 52136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	36.780578198	192.168.200.150	192.168.200.100	TCP	60	317	→ 38022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Questi sono IOC che possono indicare che qualcuno sta eseguendo una scansione dei servizi sull'indirizzo 192.168.200.150 usando la modalità TCP scan che completa il three way handshake. Infatti le porte chiuse rispondono con un pacchetto reset (RST), mentre quelle aperte che rispondono con un SYN/ACK ricevono in risposta il pacchetto ACK che completa il three way handshake.

Ci sono diverse azioni che si possono implementare per mitigare il rischio, come impostare una regola su un firewall per bloccare l'indirizzo IP sospetto, oppure implementare un IPS.

L'identificazione degli IOC è fondamentale per poter valutare le proporzioni dell'incidente e per poter attivare le procedure di incident response.