

Abbiamo osservato un elevato numero di richieste TCP ripetute, con pacchetti SYN inviati a porte diverse. Questo comportamento suggerisce che potrebbe essere in corso una scansione delle porte da parte dell'host 192.168.200.100 verso il target 192.168.200.150. Le risposte ricevute dal target confermano questa ipotesi:

Altri pacchetti hanno ricevuto una risposta [RST+ACK], segnalando che le porte sono chiuse.

Per mitigare l'impatto di questo attacco, si consiglia di configurare il firewall del target per bloccare tutte le richieste provenienti dall'IP dell'attaccante, ovvero 192.168.200.100. Questo impedirebbe all'attaccante di ottenere informazioni sulle porte e sui servizi in ascolto. In particolare, si potrebbero impostare regole firewall per:

Monitorare e registrare gli accessi per identificare e rispondere tempestivamente a future attività sospette.

Apply a dynamic filter	ICAT-15				
Time	Source	Destination	Protocol	Length	Info
118.36.776095648	192.168.200.158	192.168.200.100	TCP	60	8114 - 43160 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
119.36.776095700	192.168.200.158	192.168.200.100	TCP	60	8186 - 43080 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
120.36.776095752	192.168.200.158	192.168.200.100	TCP	60	8186 - 43074 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
121.36.776095804	192.168.200.158	192.168.200.100	TCP	60	8884 - 51282 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
123.50.776037573	192.168.200.150	192.168.200.150	TCP	74	44244 - 500 (SYN) Seq=0 Win=0 Len=0 Seq=0
123.50.77672260	192.168.200.150	192.168.200.150	TCP	74	43080 - 793 (SYN) Seq=0 Win=0 Len=0 Seq=0
124.36.776058441	192.168.200.154	192.168.200.100	TCP	60	609 - 42424 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
125.36.77611310	192.168.200.180	192.168.200.150	TCP	74	51230 - 274 (SYN) Seq=0 Win=0 Len=0 Seq=0
126.36.776045117	192.168.200.150	192.168.200.150	TCP	74	43074 - 42 (SYN) Seq=0 Win=0 Len=0 Seq=0
127.50.766035051	192.168.200.150	192.168.200.100	TCP	60	7803 - 43080 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
128.26.760121127	192.168.200.158	192.168.200.100	TCP	60	274 - 51236 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
129.36.760148673	192.168.200.150	192.168.200.150	TCP	74	57531 - 58 (SYN) Seq=0 Win=0 Len=0 Seq=0
130.36.760176331	192.168.200.150	192.168.200.150	TCP	74	48922 - 260 (SYN) Seq=0 Win=0 Len=0 Seq=0
131.36.760176317	192.168.200.150	192.168.200.150	TCP	74	48922 - 260 (SYN) Seq=0 Win=0 Len=0 Seq=0
132.26.760191700	192.168.200.150	192.168.200.150	TCP	60	68 - 57057 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
133.36.760125817	192.168.200.150	192.168.200.150	TCP	74	37470 - 11 (SYN) Seq=0 Win=0 Len=0 Seq=0
134.36.760346429	192.168.200.180	192.168.200.150	TCP	74	49640 - 230 (SYN) Seq=0 Win=0 Len=0 Seq=0
137.36.760499910	192.168.200.190	192.168.200.150	TCP	74	30540 - 729 (SYN) Seq=0 Win=0 Len=0 Seq=0
138.36.760427800	192.168.200.150	192.168.200.150	TCP	74	30604 - 58 (SYN) Seq=0 Win=0 Len=0 Seq=0
137.36.760452700	192.168.200.150	192.168.200.150	TCP	74	51210 - 998 (SYN) Seq=0 Win=0 Len=0 Seq=0
139.36.760488907	192.168.200.150	192.168.200.150	TCP	74	38813 - 817 (SYN) Seq=0 Win=0 Len=0 Seq=0
139.36.760777800	192.168.200.158	192.168.200.100	TCP	60	68 - 48922 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
140.36.760777801	192.168.200.150	192.168.200.100	TCP	60	11 - 37152 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
141.36.760776626	192.168.200.150	192.168.200.100	TCP	60	235 - 48880 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
142.36.760776816	192.168.200.150	192.168.200.150	TCP	60	779 - 35040 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
143.36.760778121	192.168.200.150	192.168.200.150	TCP	60	894 - 50904 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
144.50.760781510	192.168.200.150	192.168.200.100	TCP	60	6990 - 52136 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
145.50.760781510	192.168.200.150	192.168.200.100	TCP	60	317 - 52136 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
146.760811715	192.168.200.180	192.168.200.150	TCP	74	49444 - 961 (SYN) Seq=0 Win=0 Len=0 Seq=0
147.36.760781823	192.168.200.150	192.168.200.150	TCP	74	51210 - 241 (SYN) Seq=0 Win=0 Len=0 Seq=0
147.36.760781823	192.168.200.150	192.168.200.150	TCP	74	42541 - 233 (SYN) Seq=0 Win=0 Len=0 Seq=0
149.50.760247470	192.168.200.150	192.168.200.150	TCP	60	341 - 51210 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
150.36.760083009	192.168.200.158	192.168.200.100	TCP	60	41820 - 874 (SYN) Seq=0 Win=0 Len=0 Seq=0
151.36.760095840	192.168.200.180	192.168.200.150	TCP	74	48914 - 137 (SYN) Seq=0 Win=0 Len=0 Seq=0
152.36.761077050	192.168.200.150	192.168.200.100	TCP	60	293 - 42742 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
153.36.761144601	192.168.200.150	192.168.200.150	TCP	60	893 - 42742 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
155.36.76					

Risposte negative  
da parte dell'host. La porta è chiusa