

Threat Intelligence & IOC

In base all'analisi di Wireshark si possono notare due tipi di attacco principale:

- Reset Flood o RST Flood che tenta di interrompere le connessioni esistenti(1026 pacchetti)

No.	Time	Source	Destination	Protocol	Length	Info
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
7	23.764899991	192.168.200.100	192.168.200.150	TCP	60	33800 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810522428 TSecr=4294951105
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 -> 33876 [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
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	893 -> 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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	36.775614554	192.168.200.100	192.168.200.150	TCP	60	41304 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535438 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	60	56120 -> 111 [RST, 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	60	41182 -> 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
40	36.775917876	192.168.200.100	192.168.200.150	TCP	60	55556 -> 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
41	36.775985853	192.168.200.100	192.168.200.150	TCP	60	53602 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 -> 56884 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 -> 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 -> 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 -> 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	36.776959084	192.168.200.150	192.168.200.100	TCP	60	143 -> 33286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	36.776959882	192.168.200.150	192.168.200.100	TCP	60	110 -> 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64	36.776959162	192.168.200.150	192.168.200.100	TCP	60	580 -> 54888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
66	36.777151484	192.168.200.150	192.168.200.100	TCP	60	487 -> 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74	36.777438632	192.168.200.150	192.168.200.100	TCP	60	797 -> 56900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777438741	192.168.200.150	192.168.200.100	TCP	60	436 -> 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78	36.777623882	192.168.200.150	192.168.200.100	TCP	60	98 -> 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 -> 49760 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 -> 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 -> 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 -> 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 -> 51586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
87	36.777893298	192.168.200.150	192.168.200.150	TCP	60	33042 -> 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535441 TSecr=4294952466
88	36.777896759	192.168.200.150	192.168.200.150	TCP	60	46990 -> 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.150	192.168.200.150	TCP	60	68632 -> 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535441 TSecr=4294952466
93	36.778358546	192.168.200.150	192.168.200.150	TCP	60	148 -> 51490 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778358948	192.168.200.150	192.168.200.100	TCP	60	880 -> 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778448494	192.168.200.150	192.168.200.100	TCP	60	221 -> 51586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
99	36.778663964	192.168.200.150	192.168.200.100	TCP	60	1907 -> 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721888	192.168.200.150	192.168.200.100	TCP	60	286 -> 34640 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
103	36.778926294	192.168.200.150	192.168.200.100	TCP	60	131 -> 54202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	192 -> 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 -> 51270 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
108	36.778952310	192.168.200.150	192.168.200.100	TCP	60	656 -> 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 -> 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 -> 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- SYN Flood con spoofing delle porte si capisce perché ci sono molteplici pacchetti TCP con il flag SYN senza avere una risposta ACK(1039 pacchetti) , cambia anche le porte di origine per rendere più difficile filtrare il traffico malevolo.

No.	Time	Source	Destination	Protocol	Length	Info
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
7	23.764819289	192.168.200.100	192.168.200.150	TCP	60	33800 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810522428 TSecr=4294951105
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 -> 33876 [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	36.774691616	192.168.200.150	192.168.200.100	TCP	60	41304 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535438 TSecr=4294952466
26	36.774711972	192.168.200.150	192.168.200.100	TCP	60	56120 -> 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535438 TSecr=4294952466
29	36.775172001	192.168.200.150	192.168.200.100	TCP	60	893 -> 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
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	36.775614554	192.168.200.100	192.168.200.150	TCP	60	41304 -> 23 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535438 TSecr=4294952466
34	36.775652497	192.168.200.100	192.168.200.150	TCP	60	56120 -> 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
37	36.775983786	192.168.200.100	192.168.200.150	TCP	60	55556 -> 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
38	36.775981323	192.168.200.100	192.168.200.150	TCP	60	53602 -> 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
40	36.775985853	192.168.200.100	192.168.200.150	TCP	60	53602 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
41	36.775985853	192.168.200.100	192.168.200.150	TCP	60	53602 -> 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535439 TSecr=4294952466
47	36.776451284	192.168.200.150	192.168.200.100	TCP	60	199 -> 56884 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	36.776451357	192.168.200.150	192.168.200.100	TCP	60	995 -> 54220 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55	36.776813123	192.168.200.150	192.168.200.100	TCP	60	587 -> 34648 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58	36.776904922	192.168.200.150	192.168.200.100	TCP	60	256 -> 49814 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
60	36.776959084	192.168.200.150	192.168.200.100	TCP	60	143 -> 33286 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
62	36.776959882	192.168.200.150	192.168.200.100	TCP	60	110 -> 49654 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64	36.776959162	192.168.200.150	192.168.200.100	TCP	60	580 -> 54888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65	36.776941772	192.168.200.100	192.168.200.150	TCP	60	33042 -> 445 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535440 TSecr=4294952466
66	36.776941620	192.168.200.100	192.168.200.150	TCP	60	46990 -> 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535440 TSecr=4294952466
67	36.776962320	192.168.200.100	192.168.200.150	TCP	60	68632 -> 25 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535440 TSecr=4294952466
68	36.776983878	192.168.200.100	192.168.200.150	TCP	60	37282 -> 53 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535440 TSecr=4294952466
69	36.777118481	192.168.200.150	192.168.200.100	TCP	60	487 -> 51534 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
74	36.777438632	192.168.200.150	192.168.200.100	TCP	60	797 -> 56900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
75	36.777438741	192.168.200.150	192.168.200.100	TCP	60	436 -> 35638 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
78	36.777623882	192.168.200.150	192.168.200.100	TCP	60	98 -> 34120 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 -> 49760 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 -> 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 -> 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 -> 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 -> 51586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
87	36.777893298	192.168.200.150	192.168.200.150	TCP	60	33042 -> 445 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535441 TSecr=4294952466
88	36.777896759	192.168.200.150	192.168.200.150	TCP	60	46990 -> 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535441 TSecr=4294952466
89	36.778031265	192.168.200.150	192.168.200.150	TCP	60	68632 -> 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsval=810535441 TSecr=4294952466
93	36.778358546	192.168.200.150	192.168.200.100	TCP	60	148 -> 51490 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Da qui si evince che molto sicuramente è un attacco DDos, probabilmente l'attacco è partito con l'utilizzo di un Botnet utilizzato per reclutare una rete di computer detti "zombie" ipotizzo questa soluzione perché utilizzano un RST Flood che vuole bloccare tutte le connessioni di rete o di un'applicazione. L'unico dubbio è che l'attacco proviene da un solo indirizzo IP.

Azioni per mitigare l'attacco attuale:

- Abilitare il Rate Limiting: configurando il Firewall o router per limitare il numero di richieste SYN e RST da una singola attività
- Filtraggio dei Pacchetti Anomali: inserendo delle regole nel Firewall per rifiutare pacchetti SYN e RST non richiesti o che provengono da indirizzi IP sconosciuti
- Attivare il SYN Cookie: per ridurre l'impatto degli attacchi SYN flood
- Utilizzare un Sistema di Prevenzione delle Intrusioni (IPS): per monitorare e bloccare traffico sospetto, compresi gli attacchi SYN e RST flood.
- Contattare il Fornitore di Servizi Internet (ISP): potrebbero essere in grado di bloccare il traffico malevolo prima che raggiunga la tua rete.

Azioni per prevenire attacchi futuri:

- Implementare un Servizio di Protezione DDoS: può rilevare e mitigare attacchi su larga scala in tempo reale
- Rafforzare la Sicurezza del Server: aggiornando costantemente il sistema operativo e le app
- Monitoraggio Continuo della Rete: implementando sistemi di monitoraggio che consentono di rivelare traffico o picchi sospetti ed anomali
- Pianificare e Testare un Piano di Risposta agli Incidenti: include azioni specifiche da intraprendere in caso di attacco DDoS e simula attacchi per testare l'efficacia del piano
- Bloccare le Reti di Botnet Note: aggiornando regolarmente le liste di indirizzi IP conosciuti per essere parte di botnet e bloccarle a livello di firewall.