

# Cybersecurity Incident Report

## Section 1: Identify the type of attack that may have caused this network interruption

One potential explanation for the website's connection timeout error message is:

The logs show that: There are fer sources making a tcp syn request 198.51.100.23, 203.0.113.0, 198.51.100.14,, 198.51.100.16, 198.51.100.5 where the last 3 are from the same network. Those IP addresses are requesting a syn request using TCP protocol from 190.0.2.1. Whats obvious is that at a point HTTP protocol kick in which means that the 3 way handshake is in progres, but after few requests we see HTTP/1.1 504 Gateway Time-out (text/html) which means that the server didn't respond in time. After which we see that there are only syn requests from 203.0.113.0, and the server does not respond.

This event could be: What the conclusions can be is that this is a DoS attack using SYN flooding.

## Section 2: Explain how the attack is causing the website to malfunction

When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake:

1.

47 3.144521 198.51.100.23 192.0.2.1 TCP 42584->443 [SYN] Seq=0 Win=5792 Len=120...

This is the initial TCP Syn request to the destination port 443(HTTPS)

2.

48 3.195755 192.0.2.1 198.51.100.23 TCP 443->42584 [SYN, ACK] Seq=0 Win=5792 Len=120...

Here the server is responding to the initial SYN request, and is ready to establish connection and must receive acknowledgment from the client.

3.

49 3.246989 198.51.100.23 192.0.2.1 TCP 42584->443 [ACK] Seq=1 Win=5792 Len=120...

What happens here is that the handshake is completed and the client sends to the server's message that the acknowledgement is accepted.

Explain what happens when a malicious actor sends a large number of SYN packets all at once: First we have to explain that SYN is a 3 step process, called handshake, First the client send request to the server, the server sends answer that the request is acknowledge and then the client sends message that it has received the acknowledgment and the connection is then established. What happens is that A client or multiple clients send the initial SYN, after which the server responds, and is awaiting answer from the client, and that answer never comes, instead there are multiple new SYN packets sent, which result in slowing down or complete unavailability of the server.

Explain what the logs indicate and how that affects the server:

What's obvious from the part of the report I've passed down is that after a few successful handshakes and multiple requests the server is slowing down. After that we observe how the server responds to the SYN requests, but there is no answer to the point when the server becomes unresponsive and all we see are SYN requests from the same IP address. This Disrupts the availability which can lead to financial and reputational damage. To avoid problems like this some configurations might be altered where multiple syn request from the same place to be filtered. Or the SYB requests to be limited to certain number for a period of time. Add firewall rules that filter suspicious requests, buy DdoS antivirus software, or rent a cloud base DdoS protection.

77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	7.360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
80	7.380773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win=5792 Len=120...
81	7.380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	7.383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
83	7.482754	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
84	7.581829	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
85	7.680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0...
86	7.709377	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
87	7.738241	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
88	7.767105	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
89	13.895969	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
90	13.919832	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
91	13.943695	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
92	13.967558	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=1 Win=5792 Len=120...
93	13.991421	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
94	14.015245	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
95	14.439072	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
96	14.882899	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
97	14.888727	198.51.100.9	192.0.2.1	TCP	4631->443 [SYN] Seq=0 Win=5792 Len=0...
98	15.310554	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
99	15.734381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
100	16.158208	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
101	16.582035	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
102	17.005882	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
103	17.429878	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
104	17.452693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
105	17.475708	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
106	17.498723	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
107	17.521738	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
108	17.544753	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
109	17.567768	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
110	17.590783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
111	18.413795	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
112	18.436807	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
113	18.459819	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
114	18.482831	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
115	18.506855	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
116	18.529867	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
117	18.552879	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
118	18.575892	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
137	25.012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
138	25.335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
139	25.658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
140	25.981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
141	26.304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
142	26.628004	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
143	26.951017	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...