INCIDENT REPORT | 002 | SYN ATTACK

DETAILS

Source IP: 203.0.11.2
Cause: Flood of SYN requests to the web server.
Status: Server is not responding

The server is under a DoS attack, potentially a SYN flood, that eventually signaled the need to produce error messages while connecting to the main webpage.

Logs

- An IP (198.51.100.23) was able to successfully connect to the company's webpage.
- Another IP (203.0.113.0) attempts to connect to the company's webpage as well, but the TCP handshake is not completed.
- The same IP (203.0.113.0), begins producing incomplete SYN requests to the service provider.
- This causes a disruption within other TCP connections to the webpage.

```
73  6.230548   192.0.2.1       198.51.100.16  TCP    443->32641 [RST, ACK] Seq=0 Win=5792Len=120...
74  6.330539   203.0.113.0     192.0.2.1      TCP    54770->443 [SYN] Seq=0 Win=5792 Len=0...
75  6.330885   198.51.100.7    192.0.2.1      TCP    42584->443 [SYN] Seq=0 Win=5792 Len=0...
76  6.331231   203.0.113.0     192.0.2.1      TCP    54770->443 [SYN] Seq=0 Win=5792 Len=0...
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  7.581629   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...

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 17.005862  203.0.113.0     192.0.2.1      TCP    54770->443 [SYN] Seq=0 Win=5792 Len=0...
103 17.429678  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...
```

POTENTIAL PROBLEMS

- **A Denial of Service (DoS) attack, specifically a SYN flood request attack.**
- When a visitor attempts to connect to the web server, the request from their IP is part of the process for the TCP protocol. This is the **SYN request**.
- The web server accepts the request from the visitor's IP. In the protocol, this is the **SYN, ACK**.
- After finding out that the request has been accepted, the visitor's IP returns an acknowledgment. This is the **ACK**.

Sending that many SYN packets full of open requests to access the web server makes the server very overwhelmed.

The web server overloads while waiting for so many ACK requests.

The logs indicate two errors due to the web server becoming overloaded.

- **RST,ACK**
- **504 Gateway Time-out**