Report an Incident

We noticed that the employees can’t connect to our company website .

As a security team we use a network protocol analyzer to identify what happen when trying to connect website .

Logs show that there is a flood of syn requests that make server can’t response to legitimate employees.

This event could be DoS Attack by SYN flood attack from IP (203.0.113.0).

More details

Tcp connection should be pass three steps to establish

Syn request from user to establish connection.

[Syn-Ack] from server as acceptance to connection .

Ack from user to finish establishing the connection.

If an attacker send heavely amount of SYN requests the server become not be able to respond to legitimate users and if they send SYN request to server it response by [RESET] so employee should start to send SYN request again .