Cybersecurity Incident Report:
Network Attack Analysis

The type of attack that may have caused this network interruption:

One potential explanation for the website's connection timeout error message is a direct DoS attack. The web server is unable to respond to clients' requests, lacking the sufficient resources to respond to the volume of legitimate and malicious SYN requests. The Wireshark logs show that the company's web server received an excessive amount of SYN requests from a single IP address, "203.0.113.0" and stopped responding once overloaded with SYN requests from this address. This event could be a type of direct DoS attack by a malicious actor, called SYN flooding.

How the attack is causing the website to malfunction:

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

1. A synchronize [SYN] request, a SYN request is sent by a client attempting to connect to a server.
2. Once the server receives the synchronize [SYN] request, it will respond to the client with a SYN/ACK packet to knowledge receipt of the client's SYN request.
3. Then, once the client receives the final ACK packet, acknowledging permission to connect, a TCP connection is established.

A SYN flood attack occurs when a malicious actor sends an excessive amount of SYN packets all at once. If the amount of SYN requests is greater than the server resources available to respond to the requests and reserve for the connections, it will overwhelm the server and prevent legitimate requests from being acknowledged. As there would be no resources available for legitimate TCP connection requests.

The logs indicate that the server was initially able to handle requests as usual until they increased in volume. After a point, the server became overwhelmed and was no longer able to process the volume of visitors' SYN requests. Legitimate requests to the server have timed out and the server is unable to open new TCP connections to new visitors, who will receive a connection timeout message.

A way to prevent future direct DoS attacks would be configuring a NGFW, utilizing load balancing by distributing operations across hosts, so operations can continue if the baseline host infrastructure goes offline.