Security Incident Report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident includes DNS and HTTP.

Section 2: Document the incident

At first, the company website visitors informed the company that their systems were running slow after the company website prompted them to download a file to update their browser. After this incident, a network protocol is run at a sandbox environment where the website is tried to access and the logs are stored. The logs show that the user's browser requests connection through the DNS resolution request to the DNS server, then the DNS server forwards the website's IP address by accepting the request then the connection is next made to the website using the IP address provided by the DNS server through HTTP protocol where it is successful too. Then an HTTP/GET request is made and a file is downloaded. After executing the downloaded file, the user's browser requests another DNS resolution request to the DNS server. Now a different IP is forwarder and a connection is made to that new IP through HTTP protocol, where all the company's resources are free to public use.

Section 3: Recommend one remediation for brute force attacks

The brute force attacks can be avoided by implementing some password policies like rejecting login attempts after a few times of failed login attempt. A multi-factor authentication can be implemented to double-check the correct login identity. Password policies such as a minimum of 8 characters long password with at least one capital letter and a symbol. Implementing these password policies can be a remediation for brute force attacks.