Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol affected by the incident is the DNS protocol.

Section 2: Document the incident
We received emails from multiple customers today complaining about being given a prompt to download a browser update file after visiting the company website. Customers who downloaded and ran the file were redirected to a different site, which slowed their computers down. In response, the website owner attempted to login to the administrative panel, but was locked out. We begin the investigation by creating a sandbox environment to prevent further risk of damage to the parent server. To observe what a customer would experience, we initiate our network protocol analyzer tcpdump and visit yummyrecipesforme.com. The website loads with a prompt to download an executable file to update the web browser. Upon clicking the download and letting the file run, the website redirects us to a website called greatrecipesforme.com, which looks like the original company site. The imposter website, however, exposes company recipes for free, which are normally sold at a price, for profit.

Section 3: Recommend one remediation for brute force attacks
To prevent future brute force attacks from occurring the company must consider a few upgrades to certain domains. In regards to company policy, there needs to be a more secure password policy such as multi-factor authentication to prevent unauthorized users from accessing the company accounts of other employees. It should be made mandatory to have a password change every month or so to ensure nobody is using any default passwords that are easily compromised. A less cost-effective method is to

incorporate biometric identification to add yet another layer to security.