Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocols involved in the incident is the HTTP.

Section 2: Document the incident
Several customers contacted the website's helpdesk stating that when they visited the website, they were prompted to download and run a file that contained access to new recipes. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account. The cybersecurity analyst used a sandbox environment to open the website without impacting the company network. Then, the analyst ran tcpdump to capture the network traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would provide access to free recipes, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com). The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to add code that prompted the users to download a

malicious file disguised as a browser update. Since the website owner stated that they had been locked out of their administrator account, the team believes the attacker used a brute force attack to access the account and change the admin password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
I would recommend the enforcement of two-factor authentication (2FA) to prevent brute force attacks in the future. In the event that a malicious actor is aware of or obtains the credentials used within the company—whether these are default credentials or comply with a strong password creation policy—an additional identity verification step shall be required, utilizing either an alternative device (e.g., a hardware key) or a Time-based One-Time Password (TOTP) token.