Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol impacted in the incident is HTTP. Running tcpdump and accessing the yummyrecipiesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS and HTTP traffic log provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the user's computer using the HTTP protocol.

Section 2: Document the incident
Several customers contacted the website owner stating that when they visited the website they were prompted to download and run a file that asked them to update their browser. 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 test the website without impacting the company network. Then, the analyst ran tcpdump to capture the network and protocol traffic. The analyst was prompted to download a file claiming it would update the user's browser, accepted the download and ran it. THe browser theme redirected the analyst to a fake website (greatrecipiesforme.com) that looked identical to the original site. The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipiesforme.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 resolution for the greatrecipiesforme.com. The network traffic was then rerouted to the new IP address for the greatrecipiesforme.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
Some security measures they should implement to protect against brute force attacks are 2FA, strong password enforcements and login rate limits.