Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol impacted in the incident is HTTP. Running tcpdump and check yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in DNS/HTTP provided evidence for the next conclusion. Malicious file is sent to the user computed using HTTP protocol at the application layer.

Section 2: Document the incident
Several customers contacted the website owner, that when they visited the webbsite, they were prompted to download and run update for browser. Their personal computers have been operating slowly. The website owner trying to login into the web server but noticed they were locked out of their account. The cybersecurity analyst used a sandbox to test the website without impacting the internal network. Then the analyst ran tcpdump to capture network traffic. Analyst was prompted to download a file, accepted the download and ran it. The browser then redirected the analyst to fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com) The cybersecurity analyst inspected the tcpdump log. Once the connection was established over the HTTP, the analyst download and execute malicious file. The logs showed some changes in network traffic as the browser requested a new IP resolution for the fake website. Network traffic was rerouted to new IP address (fake). The senior cybersecurity professional analyzed the source code and discovered that an attacker had manipulated with website to add code that prompted the user to download a malicious file. The team believe, that attacker used a brute force attack to access the account and change the admin password.

Section 3: Recommend one remediation for brute force attacks
To improve you system against brute force attacks, need to implement two-factor authentication. The login part will include more requirement for users to identificate them. It could be a one-time password (OTP) or Google Authenticator. Once the user confirms their identity through credentials and OTP, they will gain access to the system.