Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident was HTTP and its associated ports. Analyzing the tcp dump shows the logs where the incident takes place in the DNS and HTTP traffic. The malicious file was downloaded by users while using the http protocol which is on the application layer in the TCP/IP model.

Section 2: Document the incident
First customers let the website owner know that the website wasn't functioning correctly. It made them download a file claiming to update their browsers. After this their PCs were slower and the website name changed. The website owner is also locked out of the web server. Cyber security analysts run the website in a sandbox environment. They download the file and analyze the network traffic using tcp dump. The website was redirected to a different fake website with every product listed for free. This website was identical in everything but name. The network traffic logs revealed the browser initiated a DNS request for the correct website and the connection was successful using HTTP protocol. The first HTTP GET request after the connection is likely the file download. After this GET request there is another DNS request for a different website, the identical fake website and all network traffic past this point is directed to the IP of this second website. The cyber security analyst reviewed the source code and found the attacker inserted a javascript function to download the file, which was pretending to be a browser update, and redirected the user to the fake website. The owner was locked out of the website which indicates the admin login username and password were compromised, likely through brute force. The downloaded file slowed down users' PCs, compromising them.

Section 3: Recommend one remediation for brute force attacks
One security practice to begin would be multi-factor authentication. Given this attack was brute force it was only successful because there was only one obstacle for the attacker to evade to gain full access to the web server and its source code. This is not practicing defense in depth, and it will be easily prevented by having another identity check for the admin account like an email code verification, or phone notification.