Security incident report

Section 1: Identify the network protocol involved in the incident
The Hypertext Transfer Protocol (HTTP) is used to send the malicious file to a user's computer. Used tcpdump when accessing the website to identify the issue and analyze the DNS and HTTP activity. Logs indicate that users are being redirected to an alternate website.

Section 2: Document the incident
A few clients contacted the organization with issues when visiting the website. Users state they received a file download that redirected them to another website that was displaying recipes for free. Users who downloaded files noticed a decrease in computer speeds as well. A tcpdump and sandbox were used to analyze the website to detect the issue. The issue that was stated by the customers was recreated in the sandbox. After the file was downloaded the user is then redirected to another website. The tcpdump indicates that the users will initially be directed to the companies website but then after the connection is established the file is downloaded. Once the file is opened users are redirected via a new DNS request to the other website. The company's website owner states that they are unable to log into the web server. The malicious user was able to enter into the server through brute force attack. Once inside they manipulated the source code to add new code that initiates the file download and prompts the users to open the file.

Section 3: Recommend one remediation for brute force attacks
Monitoring logs and creating alerts around the amount of password attempts

to the web server will help in detecting these types of incidences. Too many login attempts will alert other analysts of the attack. Login attempts should only come from authorized locations and computers approved by the organization.