Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the Hypertext transfer protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. Also, when we ran tcpdump and accessed the yummyrecipesforme.com website the corresponding tcpdump log file showed the usage of the http protocol when contacting the . The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
The issue was brought to the attention of the company when multiple customers called complaining that the website prompted them to download a file and when they did their device started running more slowly. After using a sandbox environment to further investigate the issue it was found that when connecting to the site "yummyrecipesforme.com " the user is redirected to the website "greatrecipesforme.com " where the user is prompted to download the malware.After further examining the javascript code it was found that it was altered to include some code that redirects the user.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
It is recommended to limit the number of trials a user can perform to make it harder to guess the password and to flag repeated attempts as suspicious so that security analysts can be better prepared