Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is HTTP (Hypertext Transfer Protocol). Since the issue occurred while accessing the web server for yummyrecipesforme.com, the interaction involved HTTP traffic. When analyzing the tcpdump log, it showed the usage of the HTTP protocol for the communication between the user's machine and the server. Additionally, the malicious file was transferred to the users' computers using HTTP at the application layer.

Section 2: Document the incident
Several customers contacted the website's helpdesk, reporting that when they visited yummyrecipesforme.com, they were prompted to download a file claiming to offer free recipes. After running the file, their personal computers began running slower. The website owner attempted to log into the admin panel but found they were locked out of their account. The cybersecurity analyst used a sandbox environment to open the website without impacting the company network. They ran tcpdump to capture network traffic while interacting with the website. Upon visiting the website, the analyst was prompted to download a file disguised as a browser update, accepted the download, and ran it. After executing the file, the browser redirected the analyst to a fake website, greatrecipesforme.com. The tcpdump logs showed that the browser initially requested the IP address for yummyrecipesforme.com. Once the connection was established over HTTP, the analyst downloaded and executed the file. The logs then showed a DNS request for greatrecipesforme.com, followed by redirection to the new IP address. This confirmed that the user had been redirected to the malicious site. The senior cybersecurity professional reviewed the source code and the downloaded file, discovering that an attacker had added code to the website prompting the download of the malicious file. The team suspects that a brute force attack allowed the attacker to gain access to the admin account and change the password. The malware executed on the users' machines, compromising their computers

Section 3: Recommend one remediation for brute force attacks
To prevent future brute force attacks, one security measure to implement is multi-factor authentication (MFA) for accessing the admin panel. This will require not only a password but also an additional form of authentication, such as a code sent to the admin's mobile device. This extra layer of security will help prevent unauthorized access even if the password is compromised. Additionally, enforce strong password policies, such as requiring complex passwords and regular password changes, to reduce the risk of attackers exploiting weak or default passwords. Implement account lockout mechanisms after a certain number of failed login attempts to slow down brute force attempts and deter malicious actors.