Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is HTTP. When we ran tcpdump and accessed the yummyrecipesforme.com site, the tcpdump log indicated the malicious file was being delivered to users' computers via the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers reported to the website's helpdesk that after visiting the site, they were prompted to download a file claiming to provide new recipes. After running the file, their computers began to slow down. The website owner also found themselves locked out of their web server account. The cybersecurity analyst investigated using a sandbox environment and ran tcpdump to capture network traffic while interacting with the site. After downloading and running the file, the browser redirected them to a fake website, greatrecipesforme.com. The tcpdump logs showed a shift in traffic from the legitimate site to this new IP address. Further analysis by a senior cybersecurity professional revealed that the attacker had injected malicious code into the website, causing users to download a file disguised as a browser update. It's suspected that the attacker used a brute force attack to lock out the website owner and change the admin password, compromising the end users' computers after the malicious file was executed.

Section 3: Recommend one or more remediations for brute force attacks
• Require password to be more complex • Avoid reusing previous passwords • Implement two-factor authentication