Security Incident Report

Section 1: Identify the network protocol involved in the incident
The protocol impacted in the incident is Hypertext transfer protocol (HTTP). Running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers have reported to the website owner that upon visiting the site, they were prompted to download and execute a file supposedly meant to update their browsers. Subsequently, they experienced a noticeable slowdown in their personal computers' performance. Upon attempting to access the web server, the website owner discovered they were locked out of their account. Utilizing a sandbox environment to ensure the safety of the company network, the cybersecurity analyst conducted tests on the website. Employing tcpdump to capture network and protocol traffic packets generated by interacting with the site, the analyst accepted a download claiming to update the browser and executed it. Consequently, the browser redirected to a counterfeit website (greatrecipesforme.com) that closely resembled the original site (yummyrecipesforme.com). Analyzing the tcpdump log, the cybersecurity analyst noted the initial browser request for the IP address of yummyrecipesforme.com. Upon establishing a connection via the HTTP protocol, the analyst recalled downloading and executing the file. Subsequently, the log revealed a sudden surge in network traffic as the browser sought a new IP resolution for the greatrecipesforme.com URL, which rerouted the traffic to the new IP address associated with the counterfeit website. Upon examination of the source code for the websites and the downloaded file, the senior cybersecurity professional uncovered evidence of an attacker's manipulation. Malicious code was inserted into the website, coercing users to download a file masquerading as a browser update. As the website owner reported being locked out of the administrator account, the team suspects a brute force attack facilitated the attacker's access to the account, enabling them to change the admin password. Ultimately, the execution of the malicious file led to the compromise of the end users' computers.

Section 3: Recommend one remediation for brute force attacks
The team intends to introduce two-factor authentication (2FA) as a security measure to defend against brute force attacks. This 2FA strategy involves an added step where users must verify their identity by confirming a one-time password (OTP) sent to either their email or phone. After successfully confirming their identity using their login credentials along with the OTP, users will be granted access to the system. This additional layer of authorization significantly reduces the likelihood of malicious actors succeeding in a brute force attack, as it demands extra authentication beyond typical login credentials.