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 the site yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. When we ran tcpdump and accessed the yummyrecipesforme.com website the tcpdump log file showed the usage of the http protocol when contacting the website. 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 contacted the website's helpdesk statingthat when they visited the website they were prompted to download and run a file that contained access to free recipes. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account. The cybersecurity analyst used a sandbox environment to open the website without impacting the company network. The analyst then ran tcpdump to capture the network traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would provide access to free recipes, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com). The cybersecurity analyst inspected the tcpdump log and saw that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst remembered downloading and running the file. The logs showed a sudden change in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website.

A senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst found that an attacker has manipulated the website to add code that prompted users to download a malicious file disguised as more “free recipes”. 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 download of the malicious file compromised the end users’ computers.

Section 3: Recommend one remediation for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to enforce two-factor authentication (2FA). Since the vulnerability that lead to this attack was the attacker’s ability to use a default password to log in, it’s important that we prevent unauthorized users to access the admin account and with two-factor authentication it will limit the amount of access to the account and any unauthorized users that attempt to brute force attack will not likely gain access to the system due to it requiring additional forms of authentication.