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, we know that requests to web servers for web pages involve HTTP traffic. Also, the tcpdump file showed that the malicious file is being transported to users' computer using HTTP protocol at the application layer.

Section 2: Document the incident
Our help desk received complaints from our clients that when trying to visit our website, a file has to be downloaded to have access to free recipes. And after the file is downloaded it redirects them to another website and their computer begins running slowly. The website owner tried to log in to the admin panel but he was unable to because it was locked. I used a sandbox environment to open the website without harming the company's network. Then, I ran tcpdump to capture the network traffic packets produced when trying to visit the website. I was prompted to download a file claiming it would provide access to free recipes, accepted the download and ran it. The browser then redirects me to a fake website called greatrecipesforme.com. I inspected tcpdump log and observed that the browser initially requested IP address for the yummyrecipesforme.com website. Once the connection was established over the HTTP protocol, I recalled downloading and executing the file. The logs showed a 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. Our senior cybersecurity professional analyzed the source code for the

websites and the download file. I discovered that an attacker had manipulated the website to add code that prompted the users to download a harmed file disguised as a browser update. And we now believe that the website owner can’t log in to the admin panel because the attacker used brute force attack to access the account and changed the admin’s password. The execution of the malicious file compromised the end user’s computers.

Section 3: Recommend one remediation for brute force attacks

To avoid similar attacked I recommend using 2FA. Adding another layer of security reduces the possibility of a brute force attack. Using a strong password along with a fingerprint or OTP they will gain access to the system. Any malicious actor that attempt a brute force attack will not likely gain access to the system because it requires additional authentication.

Another supportive measure is to prevent using any old passwords, since the vulnerability that lead to this attack was the attacker’s ability to use a default password to log in.