Security incident report

Section 1: Identify the network protocol involved in the incident

The protocol that is being impacted is Hypertext transfer protocol (HTTP) which is found in the application layer. Using tcpdump for the website yummyrecipesforme.com shows will help detect and access the problem. It will do this by capturing the protocol and showing traffic activity in a DNS & HTTP traffic log file. The malicious file is seen being transported to the user's computer using HTTP protocol at the application layer.

Section 2: Document the incident

Multiple customer have emailed the yummyrecipesforme's help desk. They complained that the company's website had prompted them to download a file to update their browser. The customers claimed that, after running the file, the address of the website changed and their personal computer began running slowly. The website owner then tried to login to the admin panel but was unable to.

The Cybersecurity analyst used a sandbox environment to observe the suspicious website behavior. They used a sandbox so the company network would not be impacted. The analyst ran tcpdump to capture the network and protocol traffic packets that were produced when interacting with the website. The analyst was prompted to download a file claiming that it would update the user's browser. They accepted the download and ran it. The browser then directed them to a fake website (greatrecipesforme.com) that looked identical to the original website.

After inspecting the tcpdump log it was observed that the browser initially requested the IP address for yummyrecipesforme.com website. Once a connection was established with the website over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed change in the network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new

IP address for the greatrecipesforme.com website.

The analyst discovered that an attacker had manipulated the website code to add code that prompted the users to download a malicious file. Because the website owner stated that they could not login to the admin account, it is indicated that the attacker used a brute force method to access the account and change the password.

Section 3: Recommend one remediation for brute force attacks

One security measure that is being planned to implement is two-factor authentication (2FA). This will help prevent future brute force attacks. It will do this by requiring the user to validate their identification by confirming a one time password (OTP). The OTP will be sent to their phone or email. Once the user confirms their identity with the OTP they will be granted access to the system. Any malicious actor that attempts a brute force attack will likely not be able to gain access because it requires additional authentication.