Security incident report

Section 1: Identify the network protocol involved in the incident

While using tcpdump to access the yummyrecipesforme.com the captured protocol, and traffic activity in the DNS & HTTP traffic log file shows that Hypertext Transfer Protocol was involved in this incident. The malicious file that was downloaded used HTTP protocol at the application layer.

Section 2: Document the incident

YummyRecipesForMe.com's helpdesk received complaints from customers who reported being prompted to download a file to update their browsers. These customers subsequently experienced browser redirection to the fraudulent site and noted decreased computer performance.

The Cybersecurity Analyst used a sandbox to test the website and observe the behavior and used tcpdump to capture the traffic and log the DNS and HTTP traffic. The analyst followed the prompts of the website and was required to download a file and thereafter redirected to another website (greatrecipesforme.com) a fake one of the yummyrecipesforme.com website where the paid information on the real website was offered for free.

In analyzing the tcpdump log, the analyst noticed the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. Thereafter there was a sudden change in 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.

On further investigation the analyst confirmed unauthorized access through brute force attack, since the administrator was locked out of their account. Identification of injected malicious JavaScript code in the website's source code. Discovery of a downloadable file facilitating browser redirection to the

fraudulent site.

Section 3: Recommend one remediation for brute force attacks
Due to the nature of this incident enforcing two-factor authentication so that another occurrence would not occur is recommended. Apart from password, OTP either by email, sms or phone could be added or a hard-token worn at all times by the admin can be put in place.