Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident was Hypertext Transfer Protocol (HTTP). This was concluded by running tcpdump while accessing the website yummyrecipesforme.com and reviewing the captured DNS and HTTP traffic log file. On inspecting the log, the malicious file can be observed as being transported to the users' computer using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers emailed yummyrecipesforme's helpdesk to complain that on accessing the company's website, it had prompted them to download a file to update their browsers. The customers stated that once they had run the file, the address of the website had changed, and their personal computers began to run more slowly. In response to these complains, the website owner tried to login to the admin panel but was unable to do so. The security team first created a sandboxed environment in which they could analyse the application and the suspected malicious file. They ran tcpdump before attempting to access the site. On accessing the site, the team were prompted to download the executable "browser update file" as previously reported. Once the file was downloaded and run, the URL changed from "yummyrecipesforme.com" to "greatrecipesforme.com". The site they were directed to was designed to look identical to the original, however the company's product (which is only available for purchase) was posted for free. On inspecting the tcpdump log, a DNS request can be seen for the IP address for yummyrecipesforme.com. Once the connection was successfully established using the HTTP protocol, a GET request can be seen to be made from the security teams IP address to yummyrecipes.com, after which follows what they believe to be the malicious file. After the GET request has completed, the security team noticed another DNS request, this time for greatrecipesforme.com, which returned a different IP address. After the DNS request resolved, a connection was successfully made to the

replicated website.

Since the administrator was unable to access the admin panel, the security team believe that the threat actor used a brute force attack to gain access, change the admin password and manipulate the source code of the website to include a malicious file disguised as a browser update. The execution of the malicious file then compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
One measure the security team plans to implement to defend against brute force attacks is 2 Factor Authentication (2FA). This will require users to not only provide a correct username and password combination, but also to enter a One Time Passcode (OTP) which will be sent to their device via email or phone, after which the users will be able to gain access.