Security incident report

Section 1: Identify the network protocol involved in the incident
The incident involved a significant impact on the Hypertext Transfer Protocol (HTTP). To identify the issue, a tcpdump was executed while accessing the website yummyrecipesforme.com. This allowed for the detection of the problem and the capturing of protocol and traffic activity, which were recorded in a DNS and HTTP traffic log file. Through analysis of this evidence, it was determined that the malicious file was being delivered to users' computers utilizing the HTTP protocol at the application layer.

Section 2: Document the incident
Following the incident multiple customers have emailed yummyrecipeforme's helpdesk. They were prompted to download a file to update their browsers upon visiting the website yummyrecipesforme.com. After running the downloaded file, they noticed changes in the website's address and observed slower performance on their personal computers. The cybersecurity analyst team was contacted to investigate the incident. In order to understand the suspicious behavior, a sandbox environment was set up. Using a network protocol analyzer, tcpdump, the website URL was accessed. The observed log shows that the browser initially requested the IP address for the website yummyrecipesforme.com. Once the connection with the website was established over the HTTP protocol, the security analysts downloaded the executing file. After that the log shows the sudden change in network traffic as the browser requested for a new IP address leading to greatrecipesforme.com URL, the network traffic was routed to that IP address. The security analysts analyzed the source code for the websites and the downloaded file. The analyst found that the attacker has embedded a malicious JavaScript function into the source code, which has made customers download and run a file. The file caused customers to be redirected to a fake version of the website greatrecipesforme.com. To identify how the attacker

got to the source code, the analyst recalls the owner saying that they had been locked out of their administrator account, which lead the security team to believe that the account had been broken into using brute force and changed the admin password.

Section 3: Recommend one remediation for brute force attacks
To prevent similar incidents in the future, it is recommended to implement strong password security practices, including the use of unique and regularly changed passwords. Account lockouts and brute force protection mechanisms should be employed such as enabling 2FA , a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP). Attackers that try to brute force will now have a hard time since there is additional authorization.