Security incident report

Section 1: Identify the network protocol involved in the incident
The incident has affected the Hypertext Transfer Protocol (HTTP). By running tcpdump and visiting the yummyrecipesforme.com website in order to identify the issue, record protocol, and monitor traffic activity in a DNS & HTTP traffic log file. At the application layer, it is seen that the malicious file is being transferred via the HTTP protocol to the users' PCs.

Section 2: Document the incident
Many users complained to the website owner about being asked to download and execute a file asking them to upgrade their browsers when they visited the page. Subsequently, their personal computers experienced sluggish performance. Upon attempting to access the web server, the website owner discovered they were locked out of their account. To investigate the issue without risking the company's network, the cybersecurity analyst utilized a sandbox environment to assess the website's functionality. Using tcpdump, the analyst intercepted network and protocol traffic packets generated by interacting with the site. Accepting a download prompt claiming to update the browser led the analyst to a counterfeit website (greatrecipesforme.com), mirroring the original (yummyrecipesforme.com). Analyzing the tcpdump log revealed that the browser initially sought the IP address for yummyrecipesforme.com. Upon establishing a connection via HTTP, the analyst recalled downloading and executing the file. Subsequently, the network traffic shifted abruptly as the browser requested a new IP resolution for greatrecipesforme.com, rerouting the traffic accordingly. A senior cybersecurity expert scrutinized the source code of both websites and the downloaded file. It was determined that an attacker had manipulated

the website, injecting code to prompt users to download a malicious file disguised as a browser update. Given the website owner's account lockout and subsequent password change, the team suspects a brute force attack enabled the attacker to gain access. The execution of the malicious file compromised end-users' computers.

Section 3: Recommend one remediation for brute force attacks
To mitigate the risk of brute force attacks, it is recommended that users change default passwords and implement two-factor authentication (2FA). With 2FA, users will be required to verify their identity using a one-time password (OTP) sent to their email or mobile device. This additional layer of authentication adds an extra barrier to unauthorized access attempts. Additionally, it is essential to secure the user interface (UI) to prevent the injection of malicious JavaScript code by external sources. Implementing measures such as input validation and output encoding can help safeguard against such attacks.