Security incident report

Section 1: Identify the network protocol involved in the incident
The incident affected the Hypertext Transfer Protocol (HTTP). By running tcpdump and examining the yummyrecipesforme.com website, we identified the issue. We captured protocol and traffic data, logging it in a file that revealed the evidence leading to this conclusion. The analysis showed that a malicious file was being delivered to users' computers via the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers reported to the website owner that upon visiting the site, they encountered prompts to download and run a file, instructing them to update their browsers. Subsequently, their personal computers experienced reduced performance. Attempts by the website owner to log into the web server revealed that their account had been locked. To investigate the issue without affecting the company network, the cybersecurity analyst utilized a sandbox environment. Employing tcpdump to capture network and protocol traffic packets generated by interacting with the website, the analyst downloaded and executed a file that claimed to update the browser. The browser then redirected to a deceptive website (greatrecipesforme.com), appearing identical to the original (yummyrecipesforme.com). Examining the tcpdump log, the analyst observed the browser initially requesting the IP address for yummyrecipesforme.com. After establishing a connection via the HTTP protocol, the analyst downloaded and executed the file. Subsequently, the logs displayed a sudden shift in network traffic as the browser sought a new IP resolution for greatrecipesforme.com, leading to a rerouting of network traffic to the new IP address. The senior cybersecurity professional scrutinized the source code for both

websites and the downloaded file. The analysis revealed that an attacker had manipulated the website, injecting code that prompted users to download a malicious file disguised as a browser update. Given the website owner's account lockout, the team suspects a brute force attack was employed to access the admin account and change the admin password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks

The team intends to enhance security by introducing two-factor authentication (2FA) as a safeguard against brute force attacks. The 2FA strategy involves an added step where users must verify their identity by confirming a one-time password (OTP) sent to either their email or phone. To access the system, users need to confirm their identity through both their login credentials and the OTP. This additional layer of authorization makes it unlikely for malicious actors attempting brute force attacks to gain entry to the system.