Security incident report

Section 1: Identify the network protocol involved in the incident
The incident involved the Hypertext Transfer Protocol (HTTP). By running tcpdump and accessing the website yummyrecipesforme.com, we were able to detect the issue and capture the protocol and traffic activity in a log file for DNS and HTTP traffic. This evidence led us to conclude that the malicious file was being delivered to users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Multiple customers reported to the website owner that upon visiting the site, they were prompted to download and execute a file, purportedly an update for their web browsers. The website owner attempted to log into the web server but found that their account had been locked. To investigate, a cybersecurity analyst used a sandbox environment to test the website without affecting the company network. The analyst then employed tcpdump to capture network and protocol traffic packets generated during interaction with the website. Upon being prompted to download a file that claimed to update the browser, the analyst accepted and executed it. As a result, the browser redirected the analyst to a counterfeit website (greatrecipesforme.com) that closely resembled the original (yummyrecipesforme.com). Upon inspecting the tcpdump log, the analyst noted that the browser initially sought the IP address for yummyrecipesforme.com. After establishing a connection with the website via the HTTP protocol, the analyst recalled downloading and running the file. Subsequently, the log indicated a sudden shift in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL, redirecting the traffic to its new IP address. A senior cybersecurity professional analyzed the source code of both websites and the downloaded file. The investigation revealed that an attacker had manipulated the website by inserting code that prompted users to download a malicious file disguised as a browser update. Additionally, given the website owner's report of being locked out of their administrator account, the team suspects that the attacker employed a brute force attack to gain access and

alter the admin password. The execution of the malicious file resulted in the compromise of the end users' computers.

Section 3: Recommend one remediation for brute force attacks
As a security measure to safeguard against brute force attacks, the team intends to implement two-factor authentication (2FA). This 2FA strategy will entail an extra step where users must verify their identity by entering a one-time password (OTP) sent to either their email or phone. Once the user successfully confirms their identity using their login credentials and the OTP, they will be granted access to the system. This additional layer of authorization makes it unlikely for malicious actors attempting brute force attacks to gain unauthorized access to the system.

- Kushagra Gupta