Security incident report

Section 1: Identify the network protocol involved in the incident
During the incident, the Hypertext Transfer Protocol (HTTP) was affected. To investigate and identify the issue, tcpdump was executed while accessing the website "yummyrecipesforme.com." This process helped capture the protocol and traffic activities, which were logged in a DNS & HTTP traffic log file. Through this analysis, it was determined that the malicious file was being delivered to users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Numerous customers reported contacting the website owner, expressing that upon visiting the site, they were prompted to download and run a file, claiming to update their browsers. Following this, their personal computers experienced a significant slowdown. Additionally, the website owner noticed being locked out of their account when attempting to log into the web server. To investigate the matter, a cybersecurity analyst utilized a sandbox environment to test the website without impacting the company network. The analyst then employed tcpdump to capture network and protocol traffic packets generated by interacting with the website. During this process, the analyst encountered the same file prompt, downloaded it, and executed it. As a consequence, the browser redirected them to a counterfeit website (greatrecipesforme.com), which appeared identical to the original site (yummyrecipesforme.com). Upon examining the tcpdump log, the cybersecurity analyst noted that the browser initially requested the IP address for yummyrecipesforme.com. After establishing a connection with the website through the HTTP protocol, the analyst recalled downloading and running the file. The logs indicated a sudden change in network traffic as the browser requested a new IP resolution for the URL greatrecipesforme.com, leading to the rerouting of network traffic to the new IP address associated with the counterfeit website.

Subsequently, the senior cybersecurity professional analyzed the source code of both websites and the downloaded file. This investigation revealed that an attacker had manipulated the website, adding malicious code that prompted users to download a file disguised as a browser update. The team suspects that the attacker gained access to the website owner's administrator account through a brute force attack, resulting in a password change. The execution of the malicious file then compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
To fortify their defenses against brute force attacks, the team has devised a security measure: the implementation of two-factor authentication (2FA). This 2FA plan introduces an extra step for users, where they must validate their identity by confirming a one-time password (OTP) sent to either their email or phone. By combining their regular login credentials with the OTP verification, users can gain access to the system. The inclusion of this additional authorization makes it unlikely for malicious actors attempting a brute force attack to succeed in gaining access to the system.