Security incident report

Section 1: Identify the network protocol involved in the incident

The incident pertains to the Hypertext Transfer Protocol (HTTP). By utilizing tcpdump and accessing the website "yummyrecipesforme.com," the issue was identified, and both DNS and HTTP traffic activity were captured in a log file. This evidence substantiated the conclusion that a malicious file was being conveyed to users' computers via 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 encountered a download prompt for a file, claiming to be a browser update. Subsequently, their personal computers experienced reduced performance. The website owner's attempts to log into the web server were unsuccessful, as they found themselves locked out of their account.

To investigate the matter, a cybersecurity analyst employed a sandbox environment to assess the website's behavior without affecting the company's network. The analyst then utilized tcpdump to capture network and protocol traffic packets generated by interacting with the website. During this process, the analyst intentionally downloaded and executed the purported browser update file. This action led the browser to redirect to a counterfeit website (greatrecipesforme.com), which strikingly resembled the original site (yummyrecipesforme.com).

Upon reviewing the tcpdump log, the cybersecurity analyst noted that the browser initially sought the IP address of the yummyrecipesforme.com site. Once a connection was established via the HTTP protocol, the analyst proceeded to download and run the file. Notably, the logs demonstrated a sudden shift in network traffic when the browser requested a new IP resolution, this time for the greatrecipesforme.com URL. Consequently, the network traffic was rerouted to the new IP address associated with the counterfeit greatrecipesforme.com website.

The senior cybersecurity expert delved into the source code of both websites as well as the downloaded file. This thorough analysis unveiled that an attacker had illicitly altered the website's code to insert a prompt coercing users into downloading a malicious file disguised as a browser update. Given the website owner's report of being locked out of their admin account, the team hypothesizes that the attacker might have exploited a brute force attack to compromise the account and change the admin password. The execution of the malicious file ultimately resulted in the compromise of end users' computers.

Section 3: Recommend one remediation for brute force attacks

As part of the security strategy, the team intends to introduce a safeguard against brute force attacks by implementing two-factor authentication (2FA). This 2FA approach will incorporate an extra layer of security, compelling users to verify their identity by confirming a one-time password (OTP) sent either to their email or mobile device. Once users successfully validate their identity through both their login credentials and the OTP, they will be granted access to the system. This added layer of authentication significantly diminishes the likelihood of malicious actors succeeding in a brute force attack since gaining entry to the system necessitates supplementary authorization beyond mere login attempts.