Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved was hypertext transfer protocol (HTTP) on port 80. Furthermore, the issue involves a malicious file being downloaded to user's computers at the application layer.

Section 2: Document the incident

Several customers contacted the website's helpdesk for issues with the website. When the website was visited, they were prompted to download a file containing new recipes. Their computers have been running slowly after downloading the file. The website owner tried to log into the webserver, but could not due to a password change.

A sandbox environment was used to assess the website for any malicious activity without affecting the company network. Tcpdump was used to capture the network traffic produced by interacting with the website, and a prompt to download the file that contained "new recipes." The user was redirected to a different website afterwards.

After observing the tcpdump log, it showed that the browser's initial request was to the original website. This request was over HTTP. However, after the download of the malicious file, the log showed a change in network traffic to the new malicious website.

The source code for the websites and downloaded file were analyzed and it was discovered that the malicious actor manipulated the website to add a prompt to download the malicious file for "new recipes." Because the website owner was locked out of the web server, we can conclude that the website owner's account had been accessed and the admin password had been changed by the malicious actor. Any user that downloaded the file compromised their computer.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks, stronger password requirements should be implemented. The malicious actor was able to gain access to the web server because of the use of a “default password.” Stronger password requirements and not allowing previous password use will mitigate the risk associated with brute force attacks. Stronger password requirements should encompass the use of longer passwords (at least 12 characters long), the need for upper and lowercase letters, and the need for a symbol (@#$%), Furthermore, the implementation of multifactor authentication (MFA) or two-factor authentication (2FA) will prevent future compromise of the website owner’s accounts. Access to the system will require authentication sent to the user’s phone or email address.