Security incident report

Section 1: Identify the network protocol involved in the incident

HTTP or Hypertext transfer protocol is the protocol involved in the incident. This is due to the fact that the file is being transported to the user's computers using HTTP.

Section 2: Document the incident

The incident began when clients contacted us stating that upon visiting the website, they were prompted to download a file and also took them to a site that was not our own. After which, they're devices also started to run more slowly. The website owner investigated further by attempting to log in to the admin account but was locked out. This provided evidence that our admin account was hacked by most likely a brute force attack as the admin account still had default password settings.

We then tested the client claim by using a test environment and ran tcpdump. We discovered that we were indeed prompted to download the file and run it which redirected us to the fake website called greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks

Similar attacks in the future can be prevented by strengthening our password requirements and adding additional authentication. Default passwords should be changed immediately and changed over time. In addition, there should be a warning if the wrong password is used multiple times. If a password is guessed correctly, multi factor authentication such as one time passwords or biometrics should be used to ensure malicious actors do not have access to the account.