Security incident report

By: Shihab Islam

Section 1: Identify the network protocol involved in the incident

The protocol involved in this incident is the Hypertext transfer protocol(HTTP). When using a packet sniffer to obtain the tcpdump It showed most of the traffic problems occur in the DNS. The malicious file transports people using HTTP to a different website altogether.

Section 2: Document the incident

It all started when several customers contacted the website owner stating that when they visit the website they are prompted to download a file which asked users to update browsers. Then their browsers reported to be slower as a result. FInally the website owner tried logging into an admin account but were locked out from it.

A cybersecurity analyst used a sandbox environment to isolate the website and its potential damages. After capturing a tcpdump to review the network and protocol traffic packets by the website. The analyst was prompted to download a file to update the browser. After running the download the analyst was redirected to the fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com).

The cybersecurity analyst reviewed the tcpdump log and saw the browser requested the IP address for the yummyrecipesforme.com website. Once the HTTP protocol starts it redirects here to another website which is the fake version. The IP address was redirected to this new website.

After extensive studying the analyst concluded that the had manipulated the code to add new sections to the website. It was a result of a brute force tactic, since the admin lost access to the account after the password and username changed. To which affected users computers on their ends.

Section 3: Recommend one remediation for brute force attacks

One resolution to this problem is to add measures to verify all users. One method to use is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (OTP) sent to either their email or phone. All legit users could access after verifying both but not the attacker without that credential.