Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol that was being used during this incident was HTTP protocol. We know this because the issue occurred when trying to access the web server for yummyrecipesforme.com and we know that the requests to web servers for web pages use HTTP protocols. Also after we used tcpdump and reviewed the logs we saw that the HTTP protocol was used when contacting the malicious file. The malicious file was seen being put on the user's computer using the HTTP protocol at the application layer.

Section 2: Document the incident

Helpdesk was contacted after several customers informed the help desk that they were being prompted to download and run a file that gave them more access to recipes. Customers reported that after downloading and running this file their computers were running much slower. The owner of this website then tried to log in to the website and investigate the root of the issue but found he had been locked out of his account.

Using a sandbox the cybersecurity analyst opened the company website so that the company network would not be affected. The analyst then ran the tcpdump to capture network packets. The analyst was then prompted to download and run a file that would give access to more recipes. The analyst accepted the download and ran it. The analyst was redirected to a fake website.

The cybersecurity analyst then analyzed the source code of the website. They found that the source code had been altered so that the visitors of this website would be prompted to download and run the malicious file. With the admin being locked out of this account it is safe to assume that this was a brute force attack to access the admin account and change the admin's password.

Section 3: Recommend one remediation for brute force attacks

There are a couple recommendations the team plans to implement to further prevent brute force attacks. One of them being to disallow the use of previous passwords from being used. Since the cause of this issue was due to weak password security it is important to try and eliminate the use of weak or old passwords from being used. Another security measure we will implement is password security updates more frequently. A third measure could be taken if we enable two factor authentication making it significantly harder for brute force attacks to occur. The more authentication it takes to access the admins account the harder it is for the brute force attacks to occur.