Cybersecurity Incident Report

Summary of the Problem

Clients were complaining that the website was prompting them to download a file, after the download, their computers were running significantly slower.

Analysis

Tcpdump was used to analyze the network while testing the site. When attempting to run the website, there is a request that generates that leads to the download of a malicious file. Once downloading that file, the site is redirected to “greatrecipesforme.com” which is built to look exactly like the original website. It seems that the source code of the website was altered to redirect to this malicious website that leads to the download of malware. The download was advertised as free access to the best selling recipes, which is what was enticing customers to click on it.

A brute force attack was performed. This means that the password to the admin account was not strong enough and was guessed. Once the admin account was accessed, the website was changed and so was the admin password which is why the account wasn’t accessible after this event took place. It is advised to avoid a brute force attack in the future, that stronger passwords, two-factor authentication, and a monitoring of login attempts are enforced.