Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is HTTP (Hypertext Transfer Protocol) because the issue occurred when accessing a website - yummyrecipesforme.com.

Section 2: Document the incident

When users tried visiting yummyrecipesforme.com, they would be prompted to download and run a file claiming to give them access to free recipes. This file would contain malware that would slow their PC’s afterward. The users would also be redirected to greatrecipesforme.com.

An analyst created a sandbox environment in order to test the website without affecting the company's network. They then ran a tcpdump in order to read logs of the events that occurred after attempting to visit the website yummyrecipesforme.com and were able to confirm what the users were claiming. After downloading the file, they were redirected to the fake website greatrecipesforme.com.

This was a brute force attack from a former employee who guessed one of the default admin passwords to gain entry. The issue was discovered after a few customers emailed the help desk informing them what had happened to them.

Section 3: Recommend one remediation for brute force attacks

All staff members should be using more secure passwords by having a minimum of 8 characters, one capital letter, a number, and a symbol to further prevent brute force attacks.