**31 May 2023**

**TO WHOM IT MAY CONCERN**

**SUBJECT:** Cybersecurity Incident Report

In the afternoon, I received communication from the help desk of the website yummyrecipesforme.com. Several customers had reached out complaining that the website had prompted visitors to download a run a file upon visiting the website causing their computers to run slowly and redirecting them to a different website url. The website owner had also mentioned they no longer had access to the admin panel.

I utilized a virtual machine to access the website and produce server logs using tcpdump. On the virtual machine, port 36086 was accessed and a get request was performed to yummyrecipesforme.com. A separate javascript file was loaded and a function was run, which caused my machine to send another DNS query for the domain greatrecipes.com on port 80. On the virtual machine at port 56378 a connection was made to greatrecipesforme.com. The file that was downloaded was determined to be the recipes for free.

It was determined that a disgruntled employee had brute force attacked the admin page because the website owner did not change the default password. This allowed the disgruntled employee to include a malicious javascript file that redirects users to a different webpage prompting them to download the recipe file.

Remediation for this would be to change the password policy to require a strong password, and to include two factor authentication (2FA) to ensure only the owner is logging into the admin panel.

Respectfully,

John Laffey

Cybersecurity Analyst