**Security Incident Report (1)**

**Incident Under Review:**

IT support team was notified by customer complaints of requiring them to download a file when visiting yummyrecipesforme.com that redirected them to a different website after downloading called greatrecipesforme.com. Customers also noted that their personal computers began to run slower after downloading the file.

**Network Protocols Involved:**

The network protocol impacted by this incident was the Hypertext Transfer Protocol (HTTP). This conclusion is the result of utilizing the network analyzer tcpdump while running the yummyrecipesforme.com and analyzing the log data to detect the problem and gather the evidence as to its cause.

**Documented Incident:**

The IT team was notified through customer complaints that when visiting the website, yummyrecipesforme.com, they were requested to download a file. Upon downloading the file customers were re-routed to a different website called greatrecipesforme.com that was similar in appearance to the original website but contained all recipes available for free. Customers also complained that after downloading the file their devices ran slower than they did before.

To investigate the incident a sandbox environment was utilized to conduct the investigation. Since the client’s customers complained of slower speeds this was done to avoid potential damage to the operating system. The network analyzer tcpdump was used to provide logs of the data traffic.

Logs indicated that a successful connection was first made between the user device and the DNS web server containing the correct IP address for the client’s website. A successful connection was also made between the user device and the client’s website.

Logs then indicated an HTTP request within the client’s website using the HTTP GET method (presumed the download of the mentioned file). Logs then indicate a new DNS request was initiated and a response with a new IP address was received (presumed the IP address for greatrecipesforme.com) and then the user device is rerouted to the new IP address.

Further investigation that the client’s website’s source code had been altered to include a JavaScript script that was prompting users to download the malicious file that rerouted users to the new website. Evidence suggests that the client’s web server was victim to a brute force attack as a result of a weak password being the only layer of security for the web host server.

**Security Measures to Implement:**

Moving forward it is recommended that the client institute improved policies related to accessing the web server. Improved password requirements to meet modern standards as they are significantly harder to guess as well as limits on attempted password attempts to prevent the chances of this kind of brute force attack from occurring again in the future.