Security incident report

Section 1: Identify the network protocol involved in the incident

Protocol HTTP was used by the threat actor to send the malicious download file to our clients' browsers.

Section 2: Document the incident

The incident began some hours prior 2pm. Several clients complained that the company's website had forced them to download a file to update their browsers. The file was found to be malicious and making their computers run slowly. The security response team performed a further investigation by accessing the company website from a sandbox environment. Upon accessing the website's URL the browser was prompted to download a file and let it run. Afterwards the browser redirected to a different URL, greatrecipesforme.com, which looks identical to the original website.

The logs show the following process:
1. The browser requests a DNS resolution for ymmyrecipesforme.com URL
2. The DNS replies with the correct IP address
3. The browser initiates a HTTP request for the webpage
4. The browser prompts download of the malware
5. The browser requests a new DNS resolution for greatrecipesforme.com URL
6. The DNS replies with the new IP address
7. The browser initiates a HTTP request for the webpage of the new URL

Our findings were reported to a senior security analyst. He confirms the compromise of the website and checks the source code of the website for any changes. A JS code was found to be added to prompt users to download an executable file. Analysis of the file was found to contain a script that redirects a user's browser from yummyrecipesforme.com to greatrecipesforme.com. The findings show that a bruteforce attack was made on the webserver.

Section 3: Recommend one remediation for brute force attacks
The company can reduce chances of another bruteforce attack by adding a CAPTCHA service to confirm the identity of a person before allowing for access to the website. Also, adding password policies such as limiting the number of login attempts and requiring use of strong passwords is recommended