Security incident report

Section 1: Identify the network protocol involved in the incident
Redirected DNS requests at the application layer.

Section 2: Document the incident
A malicious actor executed a brute force attack in order to: 1. gain access to the web host for yummyrecipesforme.com, 2. modify the website's source code in order to embed a javascript function 3. download an executable to customer's machines, 4. execute code to redirect traffic to a different website (greatrecipesforme.com) which simulates the original website, but hosts free versions of recipes hosted on yummyrecipesforme.com The security team was alerted to the incident after multiple customers emailed yummyrecipesforme's helpdesk complaining that the website prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. Once this behaviour was identified as suspicious, the website owner tried to log in to the admin panel but was unable to, and then reached out to the website hosting provider. In order to address the incident, the security team created a sandbox environment in order to observe the suspicious behavior. Using the network protocol analyzer tcdump, the security team was able to replicate the suspicious behaviour, and capture the relevant log events. The logs indicate the following process: 1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.

2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request for the webpage.
4. The browser initiates the download of the malware.
5. The browser requests another DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

Upon inspecting the source code for yummyrecipesforme.com, the security team was able to identify the malicious javascript code that had been added to prompt website visitors to download the executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

The security team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

Section 3: Recommend one remediation for brute force attacks
The default password for access to the web host was still in place, which may have been a contributing factor to the success of the brute force attack. In order to mitigate future occurrences of this specific type of breach, it is recommended to enable 2FA/MFA for administrator login to this website. This will add an additional layer of security to the process of authentication, reducing the ability of malicious actors to gain admin access in the future.