DNS security incident report

Section 1: Identify the network protocol involved in the incident

According to the DNS traffic log, the network protocol that was involved in this security incident was HTTP, which is used for clear-text internet communication.

Section 2: Document the incident

The threat actor used a brute force password attack to gain access to the admin page for Yummyrecipesforme.com. Once inside, he manipulated the website's source code to include a browser update that visitors would be forced to download and run; afterwards, the visitors would be redirected to Greatrecipesforme.com., a rouge website that takes proprietary recipes and makes them freely available to the public. Also the attacker disabled the admin login shortly after the DNS hijack.

Section 3: Recommend one remediation for brute force attacks

It is recommended that the organization implement two-factor authentication (2FA) to address this issue. Combining a password with a second form of authentication, such as a one-time-only access code, will make it more difficult for attackers to retrieve sensitive information in the future.