Security incident report

Section 1: Identify the network protocol involved in the incident

IP, TCP, DNS and HTTP.

Section 2: Document the incident

The website (yummyrecipesforme.com) was a victim of a successful brute-force attack, whose purpose was to lure users to a fake website with malware (greatrecipesforme.com) by adding a Javascript function to the website's source code that prompts users to download an executable file, that updates their browser and then redirects them to the malicious website; saying that is needed to access free recipes.

The data collected by using tcpdump shows that the connection between the user's computer and the actual website goes as expected, until the malicious file is downloaded and executed; then, an abnormal DNS resolution request is made from user's computer to the malicious website (greatrecipesforme.com; IP 192.0.2.172) using port .52444 to connect with the DNS server and port .56378 to connect with the spoofed website.

Section 3: Recommend one remediation for brute force attacks

Enforcing the Two-Factor Authentication(2FA).