Security incident report

Section 1: Identify the network protocol involved in the incident

Based on the provided tcpdump log, the network protocols involved in the incident include DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol). The log captures DNS requests and responses, indicating the resolution of domain names to IP addresses. Additionally, HTTP requests and responses are observed, indicating the exchange of web content between the client's machine and the yummyrecipesforme.com website initially, and later, with greatrecipesforme.com after the redirection caused by the malware.

Section 2: Document the incident

The incident involved a former employee who executed a brute force attack to gain unauthorized access to the web host of yummyrecipesforme.com. The attacker successfully guessed the correct password by repeatedly attempting several known default passwords for the administrative account, granting them access to the admin panel. Subsequently, the attacker embedded a malicious javascript function in the website's source code, which prompted visitors to download and run an executable file upon accessing the website. This file redirected users to a fake version of the website, greatrecipesforme.com, containing malware.

Multiple customers reported encountering prompts to download a file when accessing the website, resulting in their computers running slowly after executing the downloaded file. Upon investigation, it was found that the admin panel password had not been changed from the default, facilitating the success of the brute force attack. Additionally, there were no controls in place to prevent such attacks, exploiting the vulnerability of the website to unauthorized access and malicious modifications.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks in the future, implementing two-factor authentication (2FA) is recommended. Two-factor authentication adds an extra layer of security by requiring users to provide two forms of identification before granting access. It typically requires the user to enter two things: their password and a code sent to their mobile device. By implementing 2FA, even if an attacker manages to guess the password through brute force, they would still be unable to access the system without the second form of authentication, significantly reducing the likelihood of successful unauthorized access.