Security incident report

Section 1: Identify the network protocol involved in the incident

The goal of this application layer attack is to download malicious updates to the user's browser and reroute them to a fake version of yummyrecipesforme.com by manipulating HTTP and DNS queries.

Section 2: Document the incident

A furious user of yummyrecipesforme.com started a brute force attack against the web server's administrative account. The attacker changed the website's source code by accessing the admin panel after figuring out the correct password. The source code was modified to include a JavaScript function that, upon site visit, requested that users download and execute a file. Users were taken to a faked version of the website with the domain name greatrecipesforme.com after downloading the file. All of the seller's paid recipes were freely posted to this website by the attacker, and users reported that their machines slowed down after downloading the file.

After simulating the customer's actions in a virtual machine environment, the cybersecurity analyst verified that the following happens when a user visits yummyrecipesforme.com:

1. A DNS resolution of the yummyrecipesforme.com URL is requested by the browser.
2. The proper IP address is returned by the DNS.
3. The browser sends the webpage an HTTP request.
4. The virus download is started by the browser.
5. For greatrecipesforme.com, the browser asks for a different DNS resolution.
6. The new IP address is returned by the DNS server.
7. An HTTP request is sent to the new IP address by the browser.

Section 3: Recommend one remediation for brute force attacks

Later on, it was found that the admin account's default password was still in place. Establishing secure password policy for this account and the company is the best defense against brute force assaults in the future. The following specific password guidelines should be applied to this account:

1. Put strategies in place to stop a lot of unsuccessful password attempts (for example, blocking particular IP addresses after an excessive number of attempts).
2. Modify the password specifications to include a specific length and a variety of characters rather than just letters.
3. Demand frequent password changes
4. Demand multi-factor authentication or two-factor authentication (2FA or MFA).

Blocking a significant number of unsuccessful password attempts is one policy to concentrate on. Using a list of frequently used passwords, a brute force attack attempts to guess as many passwords as possible by correctly guessing an account's credentials through trial and error. Because the admin account lacked preventative measures to identify a high volume of unsuccessful password attempts, the attacker was free to guess the password as many times as they want.