Security incident report

Section 1: Identify the network protocol involved in the incident
Network protocols involved in this incident: - DNS (Determines IP of the URL) - HTTP (Establishes connection and allows data transferring)

Section 2: Document the incident
This incident was first discovered by upset customers realizing that they got redirected to a website and their computers slowed down after installing the “browser update” which was really a piece of malware. Then the owner tried logging in to the admin panel but was unable to do so. From this we can recognize that someone brute forced into the admin panel and changed the credentials. From the DNS and HTTP traffic log file we see two main sections for this incident when trying to access yummyrecipesforme.com First Part - Local computer connects to DNS for yummyrecipesforme.com - DNS responds to local computer - Local computer routed to IP address for yummyrecipesforme.com - yummyrecipesforme.com downloads file to local computer over HTTP Second Part - Run the file on the local computer - Local computer connects to DNS for greatrecipesforme.com - DNS responds to local computer - Local computer routed to IP address for greatrecipesforme.com - Able to access greatrecipesforme.com

We later found that the source code of the website was altered and a piece of malicious javascript was put into the code to download the file to the users upon loading the website. Which would then redirect the users after clicking on it to a new website that had free content on it.

The admin panel used the default password and there were no controls in place to prevent a brute force attack like this one from occurring.

Section 3: Recommend one remediation for brute force attacks
A way to prevent a brute force attack from occurring like this one would be to change the default password to a stronger password that includes a combination of letters, numbers, and symbols. Which makes it much harder to guess the password and would likely require strong computers running specialized software to try and guess the password. You can also change the new stronger password on a regular timely basis to help prevent these attacks further. This is because attackers won't have as much time to try and crack the password before a new one is already in place.