Security incident report

Section 1: Identify the network protocol involved in the incident
DNS protocol was used to resolve the IP for both (yummyrecipesforme.com and greatrecipesforme.com) and HTTP protocol was used to GET website data on port 80.

Section 2: Document the incident
the website yummyrecipesforme.com was hacked by a default admin password that was easily brute forced, then the hacker changed the javascript of the website to prompt users into installing a browser update, which installs an executable that slows the computer down and redirects users to a website that contains malware called greatrecipesforme.com. The admin can't regain access to his account, so he reached to his hosting provider.

Section 3: Recommend one remediation for brute force attacks
To prevent brute force attacks from happening again we must not allow for weak passwords or / and default passwords and we should not reuse old passwords. This will make brute forcing attacks harder and to make almost impossible is adding 2FA like OTPs, so even if the password is brute forced the attacker cant access the account without the OTP.