Security Incident Report

Section 1: Identify the network protocol involved in the incident
The primary network protocol involved in this incident is the HyperText Transfer Protocol (HTTP), evident when the browser initiates a request for the webpage and later downloads the malware. The attacker's malicious JavaScript further leverages HTTP to prompt users to download a potentially harmful executable. Lastly, the brute force attack that allowed the attacker initial access might have involved the HTTP or HTTPS protocols if it targeted the web-based admin panel directly.

Section 2: Document the incident
Multiple users informed the site's proprietor that they were encouraged to download and execute an update file upon accessing the site. Subsequently, their PCs have been lagging. The site's owner couldn't access their server account. Using a sandbox to safeguard the corporate network, tcpdump was employed to monitor the site's traffic. During this process, we were asked to download a supposed browser update, which we did. This led us to a decoy website, greatrecipesforme.com, mimicking the original, yummyrecipesforme.com. Examining the tcpdump records, it was evident that after the initial connection to yummyrecipesforme.com via HTTP, the traffic shifted, pointing to greatrecipesforme.com. After reviewing both the website's code and the downloaded file, it was found that the site was altered to trick users into downloading a harmful file under the guise of a browser update. As a result, users reported suspicious download prompts, altered website behavior, and slower computer performance. Given that the site's owner couldn't access the admin panel, it's likely that the assailant gained entry through a brute force tactic, altering the admin credentials. This deceptive file jeopardized the user devices.

Section 3: Recommend one remediation for brute force attacks
Implement a multi-factor authentication (MFA) system. By requiring users to provide at least two forms of identification before gaining access, the likelihood of unauthorized entry through brute force attempts is significantly reduced. Even if an attacker guesses or obtains the password, they would still need the second form of verification, such as a text message code, a token, or a biometric verification, to gain access.