Security incident report

Section 1: Identify the network protocol involved in the incident
Two key network protocols were identified: DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol). DNS is crucial for resolving domain names into IP addresses. The logs indicate that when the user's browser requested the resolution of yummyrecipesforme.com, DNS provided the correct IP address. This process was repeated for the malicious site greatrecipesforme.com, directing the user's browser to a different IP address. This redirection is a classic example of DNS manipulation commonly used in phishing attacks. HTTP, the protocol used for transmitting web pages on the internet, was also central to this incident. The logs show the browser initiating HTTP requests to both yummyrecipesforme.com and later to greatrecipesforme.com. The attacker leveraged HTTP to serve the malicious website and facilitate the unauthorized download of the malware.

Section 2: Document the incident
Customers of yummyrecipesforme.com contacted the website owner to report an issue. They experienced prompts to download and run a file for a supposed browser update while visiting the website. Following this, their personal computers began operating more slowly. The website owner attempted to log into the web server but discovered they were locked out of their administrator account. A cybersecurity analyst at the company then used a sandbox environment to safely examine the website without risking the company's network. They employed tcpdump, a network packet capture tool, to monitor the data and protocol traffic while interacting with the website. During this process, the analyst received a prompt to download a file claiming to update the user’s browser. They downloaded and executed the file, which subsequently redirected their browser to a counterfeit website, greatrecipesforme.com, that closely resembled the original site. Upon reviewing the tcpdump log, it was observed that the analyst’s browser initially requested the IP address for yummyrecipesforme.com. This connection was established over HTTP, a standard web protocol. Following the execution of the downloaded file, the logs indicated a notable change in network traffic. The browser requested a new IP resolution for greatrecipesforme.com and was rerouted to this new address.

A senior cybersecurity professional examined the source code of both websites and the downloaded file. They discovered that the original website's code had been altered to prompt users to download a malicious file, masquerading as a browser update. Given that the website owner was unable to access their administrator account, it was inferred that the attacker utilized a brute force attack to gain entry and change the admin password. The execution of the malicious file on the end users' computers resulted in compromised system performance.

Section 3: Recommend one remediation for brute force attacks
To enhance security and prevent such brute force attacks in the future, I recommend implementing account lockout policies and multi-factor authentication (MFA). Account lockout policies would temporarily lock an account after several failed login attempts, hindering continuous password guessing attempts. MFA adds an extra security layer, requiring a second verification form, such as a code sent to a phone, even if the password is compromised. Additionally, regular password updates, rate limiting for login attempts, and vigilant monitoring of unusual login activities can further bolster our website's security.