Security incident report

Section 1: Identify the network protocol involved in the incident
The incident involves the HTTP protocol (as far as we know). Since the issue occurred while accessing *yummyrecipesforme.com*, requests to web servers use HTTP traffic. *Tcpdump* logs show HTTP usage, with the malicious file being transferred to users' computers via HTTP at the application layer.

Section 2: Document the incident
Customers reported being prompted to download a file from a website that caused their computers to slow down. The website owner was locked out of their admin account. The IT team used a sandbox and *tcpdump* to trace the network traffic, finding that the site redirected users to a fake website after they downloaded a malicious file. The attacker had injected code to prompt the download, likely after gaining admin access via a brute force attack.

Section 3: Recommend one remediation for brute force attacks
I think that the most convenient solution for these kinds of attacks is to implement a MFA to prevent unauthorized access from brute force attacks. That way, only authorized users can make use of the intended system.