Security incident report

Section 1: Identify the network protocol involved in the incident
The primary network protocols involved in this incident are the Domain Name System (DNS) and Hypertext Transfer Protocol (HTTP). DNS is used to resolve domain names into IP addresses, enabling browsers to locate and access websites. HTTP is used for communication between the client (user's browser) and the web server, allowing the transfer of web pages and other resources. During the attack, DNS was responsible for resolving the domains yummyrecipesforme.com and greatrecipesforme.com, while HTTP facilitated the communication that led to the malicious file download and the subsequent redirection to the fake website.

Section 2: Document the incident
The incident began when a disgruntled former employee executed a brute force attack to gain unauthorized access to the admin panel of yummyrecipesforme.com by guessing the default administrative password. Once inside, the attacker embedded malicious JavaScript into the website's source code. This script prompted visitors to download a file that appeared to be a browser update. Upon executing this file, users were redirected to a fake website, greatrecipesforme.com, which contained malware. This sequence of events was confirmed through analysis using a network protocol analyzer , which captured the DNS and HTTP requests leading to the download and redirection. Customers reported issues, including slow computer performance and unexpected website redirects, prompting the investigation and subsequent discovery of the breach.

Section 3: Recommend one remediation for brute force attacks
To prevent future brute force attacks, it is recommended to implement account

lockout policies. Additionally, enforcing strong password policies, such as requiring complex passwords and regular password changes, can further mitigate this threat. Employing multi-factor authentication (MFA) can add an extra layer of security, making unauthorized access much more difficult.