Security incident report

Section 1: Identify the network protocol involved in the incident
The DNS & HTTP traffic log indicates that the network protocol impacted in the incident is Hypertext transfer protocol (HTTP). The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Multiple customers emailed the company's helpdesk stating that the company's website had prompted them to download a file to update their browsers. The customers' computers have begun running more slowly since running the file and the address of the website changed. The website owner has been unable to log into the web server and was locked out of their account. The cybersecurity analyst tested the website using a sandbox environment and ran tcpdump to capture the network and protocol traffic packets produced when attempting to access the website. The analyst was prompted to download a file claiming to update their browser, accepted the download and ran it. The browser then redirected the analyst to a fake website that looked identical to the original site and had a different url. The tcpdump log showed that the browser requested a DNS resolution for the real company website's URL (yummyrecipesforme.com). After the DNS replied with the correct IP address, the browser initiated an HTTP request for the webpage and then the browser initiated the download of the malware. The browser then requested another DNS resolution for a different website (greatrecipesforme.com) and the DNS server responded with the new IP address and an HTTP request was initiated by the browser for the new IP address. The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to add code that prompted the users to download a malicious file disguised as a browser update. Since the website owner stated that they had been locked out of their admin account, the team believes the attacker used a brute force attack to access

the account and change the admin password. The execution of the malicious file compromised the end users' computer.

Section 3: Recommend one remediation for brute force attacks
One remediation recommendation to protect against brute force attacks is multi-factor authentication (MFA). MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. This verification happens using a combination of authentication factors: a username and password, fingerprints, facial recognition, or a one-time password (OTP) sent to a phone number or email. Malicious actors attempting brute-force attacks will likely not gain access to the system because it requires additional authorization.