Security Incident eport

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is HTTP (Hypertext Transfer Protocol). Since the issue occurred while accessing the web server for yummyrecipesforme.com, it confirms that web page requests use HTTP traffic. Additionally, when we ran tcpdump and accessed the website, the tcpdump log confirmed the use of HTTP. The malicious file was also delivered to users' computers via the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers reported to the website's helpdesk that, upon visiting the site, they were prompted to download a file offering access to new recipes. After running the file, their personal computers began operating slowly. Meanwhile, the website owner discovered they were locked out of their admin account. To investigate, a cybersecurity analyst accessed the website in a sandbox environment to avoid affecting the company network. Using tcpdump, the analyst captured network traffic while interacting with the site. Upon visiting the site, the analyst was prompted to download a file claiming to provide free recipes. After downloading and running it, the browser redirected to a fake website, greatrecipesforme.com. The tcpdump logs revealed that the browser initially connected to the yummyrecipesforme.com server using HTTP. After the file was executed, network traffic shifted as the browser requested a new IP address associated with greatrecipesforme.com. The traffic was then rerouted to this fake site. A senior cybersecurity professional analyzed the website's source code and the downloaded file, uncovering malicious code added by an attacker. This code prompted users to download a file disguised as a browser update. The team believes the attacker used a brute force attack to access the admin

account, change the password, and upload the malicious code. As a result, executing the file compromised users' computers.

Section 3: Recommend one remediation for brute force attacks

To protect against brute force attacks, the team plans to implement several security measures. First, they will prevent the reuse of previous passwords, including default passwords, to ensure old credentials cannot be exploited. This addresses the vulnerability that allowed the attacker to log in using a default password.

Additionally, the team should require more frequent password updates. This reduces the risk of unauthorized access since any compromised passwords will become obsolete more quickly.

Finally, the team should implement two-factor authentication (2FA). This requires users to verify their identity with both a password and a one-time passcode (OTP) sent to their email or phone. With 2FA in place, malicious actors attempting brute force attacks are unlikely to gain access, as additional authentication is required beyond just the password.