Security incident report

Section 1: Identify the network protocol involved in the incident
The incident involved the following network protocols: **DNS (Domain Name System):** The browser initiated a DNS resolution for the yummyrecipesforme.com URL. The DNS server replied with the correct IP address. Another DNS resolution was requested for greatrecipesforme.com, and the DNS server responded with the new IP address. **HTTP (Hypertext Transfer Protocol):** The browser initiated an HTTP request for the webpage from yummyrecipesforme.com. The browser initiated an HTTP request to the new IP address (greatrecipesforme.com) after the download of the malware.

Section 2: Document the incident
Several customers contacted the website owner stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account. The cybersecurity analyst used a sandbox environment to test the website without impacting the company network. Then, the analyst ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user's browser, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com).

The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website.

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 administrator 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' computers.

Section 3: Recommend remediation for brute force attacks
We can use many techniques to prevent brute force attacks in the near future this may include using the following operations to web hosts login: 1)Multi-Factor Authentication 2)Reducing the login attempts 3)Using strong passwords rather than default ones 4)Constantly monitoring for login attempts