Activity: Security Incident Report

Scenario
You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A former employee has decided to lure users to a fake website with malware.

In response to a cybersecurity incident at yummyrecipesforme.com, where a former employee exploited a brute force attack to access the admin panel and embed malware, customers reported being redirected to a malicious website after downloading a file from the compromised site. Following the incident, as a cybersecurity analyst you initiated an investigation by setting up a sandbox environment to monitor suspicious activity on the website and used network analysis tools like tcpdump. Upon visiting yummyrecipesforme.com, they were prompted to download an executable file, which led to redirection to greatrecipesforme.com, a site hosting malware.
The logs show the following process:

- The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server.
- The DNS replies with the correct IP address.
- The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server.
- The browser initiates the download of the malware.
- The browser initiates a DNS request for greatrecipesforme.com.
- The DNS server responds with the IP address for greatrecipesforme.com.
- The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

A senior analyst verified that the website was compromised after discovering JavaScript code embedded in its source, which prompted visitors to download an executable file. Further investigation revealed that the downloaded file contained a script redirecting users from yummyrecipesforme.com to greatrecipesforme.com. The cybersecurity team determined that the web server had been affected by a brute force attack. The attack succeeded due to the admin password being left at its default setting, with no safeguards in place against brute force attempts.

Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident is the Hypertext transfer protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. Also, when we ran tcpdump and accessed the yummyrecipesforme.com website the corresponding tcpdump log file showed the usage of the http protocol when contacting the website. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
Several customers contacted the website's helpdesk stating that when they visited the website, they were prompted to download and run a file that contained access to new recipes. 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 open the website without impacting the company network. Then, the analyst ran tcpdump to capture the network traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would provide access to free recipes, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.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 address 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 one or more remediations for brute force attacks
One security measure the team plans to implement to protect against brute force attacks is to disallow previous passwords from being used. Since the vulnerability that lead to this attack was the attacker's ability to use a default password to log in, it's important that we prevent any old passwords such as default passwords from being used to reset the password. Another supportive measure is to require more frequent password updates, so in case any unauthorized person becomes aware of the password, they are less likely to be able to use that password if the password is updated sooner than later. Finally, another helpful solution is to implement two-factor authentication (2FA). 2FA requires authentication via a password and also by confirming a one-time passcode (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authentication.