Security incident report

Section 1: Identify the network protocol involved in the incident

As we observed from the tcpdump traffic logs, we found out that the following network protocols were used:

1. DNS protocol : used to translate the domain name to the IP address which is used to communicate between machines.
2. HTTP protocol : To access the web server of yummyrecipesforme.com. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.
3. TCP protocol : this protocol was used to create a connection between the server and the user, it is evident from the log file as there are [S],[S.],[.] flags which indicate Synchronize, Synchronize-acknowledge, Acknowledged respectively.

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 remediation for brute force attacks

Some security measures to prevent from brute force attack:

1. Limiting the number of login attempts- This will stop the attacker from trying to login several times using the brute force method.
2. Change default password policy- After the initial login of the administrator, the password needs to be changed, which was not done in this scenario, making it more prone to the attack as default passwords are predictable.
3. Strong Password policy should be maintained- This policy will make the password strong using special characters, numbers, etc.
4. Enforcing 2FA(Two-Factor Authentication)- This will need another authenticator factor like OTP(One-Time-Password) which can only be served by the authenticated user.