Security incident report

Section 1: Identify the network protocol involved in the incident

IT team used network protocol analyzer tcpdump to analyze the network traffic. The team found out that HTTP network protocol were involved in the incident using port 80.

Section 2: Document the incident

- Around 2:30 this afternoon, the IT team started to get complaints from the customers about being unable to access the company's website yummyrecipesforme.com. They shared how they were asked to download a file when they were trying to access the company's website which would take them to a different website which greatly resemble the company's website and has free access to company's recipes and it also caused the customers' computers to runslow.
- After the complaints from the customer, our IT team started to investigate the problem. The team used network protocol analyzer tool tcpdump to monitor the network traffic in a sandbox environment.
- Upon analyzing the data, the team found out at 2:18 PM while accessing the website the browser on the company device was requesting download file via HTTP protocol.
- The team noted that 2 minutes after the download another DNS request was initiated for the website at 2:20 PM using port 52444 which was responded with IP address that was different from the prior requests. After this, the traffic changes route to the different website i.e., greatrecipesforyou.com.
- After analysing the incident, one of the senior analyst concluded that website was compromised. The source code of website was altered and embedded with javascript to download the executable file which was the reason for redirecting of traffic from company's website to the new website.
- The cybersecurity team concluded that the web server was impacted by a brute force attack.

Section 3: Recommend one remediation for brute force attacks
The investigation concluded that the attack took place because a disgruntled employee was able to guess the admin password for the website and alter the site’s code. It also pointed out that company lacked clear password policies. It would be strongly advisable to implement a strong password policy to prevent the similar future incicents.