Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident is:

- HTTP
  - The traffic captured in the log shows HTTP communication between the client machine (your.machine) and the servers of two different domains (yummyrecipesforme.com and greatrecipesforme.com) on port 80, which is the default port used for HTTP communication. The log includes HTTP GET requests from the client machine to retrieve the home pages ("/") of both domains, followed by the servers' responses to these requests.
- DNS
  - The log also shows DNS (Domain Name System) communication between the client machine and dns.google.domain (presumably a Google DNS server) for domain name resolution. DNS is used to translate domain names (e.g., yummyrecipesforme.com) to IP addresses (e.g., 203.0.113.22) so that the client machine can communicate with the respective servers.

Overall, the network traffic involves HTTP for web communication and DNS for domain name resolution.

Section 2: Document the incident

Multiple customers emailed yummyrecipesforme’s helpdesk. They complained that the company’s website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.

A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that JavaScript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

The cybersecurity team reports that the web server was impacted by a brute-force attack, The baker executed a brute-force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one.

After they obtained the login credentials, they were able to access the admin panel and change the website's source code.

They embedded a JavaScript function in the source code that prompted visitors to download and run a file upon visiting the website.

After running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free.

Section 3: Recommend one remediation for brute force attacks

1. Change Administrative Password: Immediately change the administrative password to a strong, unique, and complex password to prevent unauthorized access.
2. Implement Brute Force Protection: Set up measures, such as account lockout policies or rate limiting, to prevent brute force attacks on the admin panel.
3. Security Monitoring: Deploy intrusion detection/prevention systems to monitor and identify suspicious activities in real-time.
4. Code Review: Conduct a thorough code review of the website to identify and remove any injected malicious code.
5. Regular Security Audits: Conduct regular security audits to identify and fix potential vulnerabilities in the website's infrastructure and source code.