Security incident report

Section 1: Identify the network protocol involved in the incident

After analysing the tcpdump log and attempting to visit the website, it was confirmed that the incident occurred at the application layer specifically involving the Hypertext transfer protocol (HTTP).

Section 2: Document the incident

Multiple customers emailed yummyrecipesforme’s helpdesk complaining that when they attempted to visit the website they were asked to download and run to allegedly update their browser a file after they ran the file it redirected them to **“greatrecipesforme.com”** and they also noticed that their computers began running more slowly. The website owner tried to log in to the admin panel but discovered that the password to the administrative account was changed.

To investigate this incident i created a sandbox environment and ran the network protocol analyzer tcpdump and typed the website URL **“yummyrecipesforme.com”** As soon as the website loads, i was prompted to download an executable file to update my browser.After accepting the download and allowing the file to run i was redirected to the URL **“greatrecipesforme.com”** which contained malware.

After reviewing the tcpdump log what happened was:

1. My computer used **Port 52444** to send a DNS resolution request to the DNS server (dns.google.domain) for the destination URL “yummyrecipesforme.com”.
2. The DNS server replied with the IP address of the destination URL **(203.0.113.22).**
3. My computer then sent a connection request using **Port 36086** directly to the destination **“yummyrecipesforme.com.http”**.
4. The destination replied acknowledging that it received the connection request

5. Then the log shows that my browser requested data from **"yummyrecipesforme.com"** with the HTTP: GET method using HTTP protocol version 1.1. Most likely the download request.
6. Then after approximately 2 minutes a sudden change happened as my computer used **Port 52444** to send a DNS resolution request to the DNS server **(dns.google.domain)** again but this time the DNS server routes the traffic to a new IP address **(192.0.2.17)** and its associated URL **(greatrecipesforme.com.http).**
7. Incoming traffic occurred from **"greatrecipesforme.com.http"** to my computer through **Port 56378.**

Given the fact that the website owner claims that he can't access the administrative account due to the password being changed implies that the attacker used brute force attack to gain access to the account then changed the source code to prompted the user to download malicious file disguised as a browser update then change the password so that the account can't be accessed.

Section 3: Recommend one remediation for brute force attacks

To prevent future brute-force attacks, enforce two-factor authentication (2FA) for all administrative accounts to require identity verification beyond passwords (e.g., time-based one-time passwords). Revise password policies to eliminate default credentials and mandate strong initial passwords (12+ characters, complexity). Supplement with rate-limiting (lock accounts after 5 failed attempts) and IP allowlisting for administrative access.