Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in this incident is the HTTPS protocol at the application layer as we noticed that the tcpdump log file showed usage of https protocol when responding to customers.

Section 2: Document the incident
A former employee had embedded a javascript function in the source code of the company's website as confirmed by a Senior Analyst. This code prompts customers to download a file containing "free recipes", and redirects them to a different URL which contains malware that slows down the computer. The incident is believed to be a brute force attack where the former employee was able to correctly guess the admin password as it was still set to the default password. The incident occurred around 2:18 pm. The Cybersecurity Analyst used a sandbox environment to open the website. We noticed that after accessing the website, we are redirected to a different URL "greatrecipesforme.com.http", a spoofed/fake website, after being prompted to download a file claiming to have "free recipes". The Cybersecurity Analyst then inspected the packet analyzer tool, tcpdump, to check the logs and saw that the browser at first initiates a DNS request for the legitimate website, which the DNS replied correctly. The browser then initiates a HTTP request using the IP address sent by the DNS server, however it then initiates a download of the malware. The network traffic is then redirected to the new IP address for the fake website.

Section 3: Recommend one remediation for brute force attacks
We recommend that the company require more frequent password changes for all employees and admin account of the website, preferably every 6 months. Another method would be to implement the limiting of number of login attempts, this can significantly reduce the chance of a successful brute force attack. Aside from that, passwords for all accounts owned by the company has to be strong, by containing at least special characters, numerals, alphabets and length of at least 8 characters.

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```