Security incident report

Section 1: Identify the network protocol involved in the incident

Communication Protocols : http - Hypertext Transfer Protocol.

Section 2: Document the incident

Company's website yummyrecipesforme.com that had prompted customers to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed to greatrecipesforme.com and their personal computers began running more slowly.

Analysis :
They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After embedding the malware, the hacker changed the password to the administrative account. When customers download the file, they are redirected to a fake version of the website that contains the malware.

To address the incident, Security Analyst creates a sandbox environment to observe the suspicious website behavior. Analyst ran the network protocol analyzer tcpdump for yummyrecipesforme.com and are prompted to download an executable file to update the browser. Analyst accepted the download and allow the file to run. We then observe that our browser redirects analyst to a fake website greatrecipesforme.com, which contains the malware.

Section 3: Recommend one remediation for brute force attacks

Enforcing two-factor authentication (2FA) - It requires a password confirmation thru OTP sending either phone or email. It prevents brute force attacks from hackers who would not be able to gain access to the system.