Security incident report

Section 1: Identify the network protocol involved in the incident

The incident occurred through HTTP protocol — an unencrypted protocol.

Section 2: Document the incident

This occurrence starts with a client accessing yummyrecipesforme.com . The client first requests the DNS for this website through google's DNS lookup tables. Google's DNS service responds with the IP 203.0.133.22 .

The client accesses the website yummyrecipesforme.com (now with the IP of the server) and starts a TCP connection sending a SYN packet [S]. The server acknowledges the connection and sends a SYN/ACK placket [S.]. The client send a ACK packet acknowledging the connection[.] and requests the index page (GET / HTTP 1.1) sending a packet ready for Data Push [P]. The server responds sending the requested page [.].

After receiving the Data Requested from the server the client (unknowingly) is redirected to the greatrecipesforme.com website, again, requesting the DNS through Google's DNS service, starting another TCP connection with this new website receiving the data requested (the index page).

After the client is redirected to the mirror page, made by the malicious actor, the client is prompted to download a file [FREE RECIPES] containing malware, compromising the client's machine.

Section 3: Recommend one remediation for brute force attacks

Due to the origin of this attack (The former employee/ hacker executed a brute force attack to gain access to the web host) it is recommend to implement a password management system, requiring stronger password policies, multi-factor authentication (MFA), requiring frequent password changes and disallowing previous password from being used. It is also recommended to implement SIEM tools to monitor and alert login attempts and to limit the amount of failed login attempts to prevent brute force attacks.