Security incident report

Section 1: Identify the network protocol involved in the incident
The protocol involved in the incident was HTTP 1.1

Section 2: Document the incident
The incident came into light when multiple customers complained at the helpdesk that when trying to access the company's website they are prompted to download a supposed "browser update", upon installation of the suspicious update they were redirected to an identical website where all the company's recipe were available for free and they observed a performance drop in their personal computers. The prompt to download an update and the redirection to a strikingly similar website seemed highly suspicious. The website owner tried to login into the website's admin panel but was unable to do so and thus contacted us. Upon investigating the incident in the sandbox environment the network analysis logs indicated: ● The request to resolve the company's domain name **yourfavoriterecipes.com** was sent from port 52444 and DNS replied with the IP address indicating a successful domain name resolution. ● Then the connection request from port 36086 was sent to the destination on port 80. ● The connection was open for 2 minutes and during this interval there was unusually high traffic on port 80. ● After the 2 minute mark a suspicious HTTP GET request was sent from the source to the destination. ● A DNS request from port 52444 was sent from the source and the DNS server responded with an entirely different IP address of 192.0.2.172 and the domain name as **greatrecipes.com**.

While investigating the issue in a sandbox a senior analyst confirmed that the website was compromised and when they inspected the source code they found a javascript code that was injected into the website's source code which was prompting users to download a browser update.

The cybersecurity team reported that the web server fell victim to a brute-force attack carried out by a disgruntled employee of the company. The attacker executed a bruteforce attack on the web host and gained access to the administrative account then logged in to the admin panel, changed the source code and injected the malicious javascript code.

Section 3: Recommend one remediation for brute force attacks
The bruteforce attack can be countered by implementing strong password policies and using multifactor authentication.