# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Two protocols are involved in this incident as they are HTTP protocol & DNS protocol. While running tcpdump we get to know that first it is using DNS to get the ip address for yumyumcookingforme.com and using HTTP to connect to it. The malicious file was noticed being sent to users' computers using the HTTP protocol at the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| Several customers reported encountering issues on the website where they were prompted to download a file, supposedly for a browser update. After doing so, their computers began operating slowly. The website owner faced a lockout from their account when attempting to log in.  To investigate, a cybersecurity analyst used a sandbox environment to test the website without affecting the company network. Running tcpdump to capture network and protocol traffic, the analyst downloaded a file, thinking it would update the browser. Instead, the browser redirected to a fake website (greatrecipesforme.com) resembling the original (yummyrecipesforme.com).  Analyzing the tcpdump log, the analyst noted the browser initially requested the IP address for yummyrecipesforme.com. Once connected over HTTP, the file download caused a shift in network traffic, leading to a new IP resolution for greatrecipesforme.com.  A senior cybersecurity professional delved into the source code for both websites and the downloaded file. They uncovered an attacker's manipulation, inserting code that tricked users into downloading a malicious file disguised as a browser update. Given the owner's account lockout, the team suspects a brute force attack granted the attacker access to the admin account, enabling a password change and compromising end users' computers. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To beef up security and guard against brute force attacks, the team is gearing up to implement two-factor authentication (2FA). This plan involves an extra layer of user verification, requiring them to confirm their identity with a one-time password (OTP) sent to either their email or phone. Once users authenticate with both their login credentials and the OTP, they'll be granted access to the system. This additional step acts as a formidable barrier, making it highly unlikely for any malicious actor attempting a brute force attack to gain unauthorized access. |