# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved in the incident is the Hypertext Transfer Protocol. After running tcpdump, the DNS & HTTP log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users’ computers using the HTTP protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers contacted the website owner stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. The customers claimed that after running the file, their personal computers began running slowly and the address of the website changed. In response to the incident, the website owner tried logging into the web server, but he was unable to.  The cybersecurity analyst created a sandbox environment to observe suspicious website behavior. Then, the analyst ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user’s browser. He accepted the download and ran it. The analyst then observed that the browser redirected him to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com).  The senior cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One security measure the team plans to implement to protect against brute force attacks is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (OTP) sent to either their email or phone. Once the user confirms their identity through this process, they will gain access to the  system. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization. |