# Security incident report

[Tcpdump traffic log](https://docs.google.com/document/d/1BWyS3v8O9kmoSLvGBRqp-R6qRAvf1v6x36KujQyL49Y/edit?usp=sharing)

[Instructions on how to read traffic log](https://docs.google.com/document/d/1yVYEJiVtcCYZ5wNhs7IBD_ik3R4XtzDTSQQeU1jSbsU/edit?usp=sharing)

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol in this incident was the HTTP, hypertext transfer protocol. We know this because the issue is with accessing the web server for the website as well as when we looked at the tcpdump log file. | |
|

| **Section 2: Document the incident** |
| --- |
| Customers were prompted to download and run a file after visiting the website. They were directed to a new website as well. They noticed that the computers ran much more slowly after this. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| One remediation for brute force attacks includes making sure to use two-factor authentication (2FA) which allows for more security. The user can only log in after confirmation with a sent code or OTP. Since there is an additional level of authentication that is required to log in, any false actors will not be able to get past the second stage of authentication needed. |