# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol involved in the incident was HTTP as the issue was with accessing the yummyrecipesforme.com website. In reviewing the tcpdump file, we saw various HTTP requests to the same website as well as a malious file being downloaded to users computers. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers reported an issue after going to the website they would be prompted to download a file and once the file was downloaded the address of the website changed and their computers ran slowly.  Cybersecurity analysts investigated further and via a sandbox environment, observed and confirmed the reported behaivior. The analysts then checked the source code and confirmed that javascript has been added to prompt website visitors to download an executable file. It was confirmed to have been a brute-force attack by a disgruntled hacker. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Recommend to enable stricter password protocols such as enabling 2FA / MFA. This would help avoid brute-force password attacks and make accounts more secure. |