# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| TCP and HTTP is used in the incident | |
|

| **Section 2: Document the incident** |
| --- |
| 14:18:32.192571, the computer first requests DNS to google, obtaining the IP address of [yummyrecipesforme.com](http://yummyrecipesforme.com).  Then, the computer makes a connection with the website.  14:18:36.786589, the computer sends HTTP GET request to the website indicating that it is downloading something, in this case a malicious program.  14:20:32.192571, now the computer requests a DNS query again to google, but this time for [greatrecipesforme.com](http://greatrecipesforme.com).  14:25:29.576493, the computer makes connection to the other website indicating that the user is accessing a fake version of the website. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Brute force attacks are often done using dictionaries.  One of the best ways to avoid those attacks are to use more secure passwords, enforcing strict rules such as length, special characters, and a frequent password change interval.  2FA is also highly recommended. It is possible to detect if the password has been breached but the attacker still has no access to it. |