# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The compromised network protocol is the HTTP. From the Tcp dump and log analysis , it can be seen that a malicious file is being transported to the users computer using the HTTP protocol |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers contacted the website owner that when they visited the website they were prompted to download a file which asked them to update their browser. After doing this their computer has been slow since then . The website owner tried to log into the web server but the passwords have been changed.  The cyber security analyst used a sandbox environment to test the website then ran tcp dump. The analyst was prompted like other users to to update their browser. He downloaded and ran it. The browser redirected the analyst to a fake or cloned website getrecipesforme.com where downloads were for free.  Upon inspection of the tcp dumps , it was found out that the browser initially requested ip address for yummyrecipesforme.com. Once the connection was established , it prompted to download a file to update this . After downloading the file, a new traffic was noticed over the HTTP protocol. The browser requested for a new ip address different from the initial one .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** |
| Password policies should be putin place. The more the characters of a password the harder it is to crack. The password should contain Upper letter, lower letters and special characters and it must not be less than 12 characters  Multi factor authentication should also be put in place . It provides an additional layer of authentication . |