# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The potential explanation is the clients were stealing it with a embed package in the website, this script is foreign to the company. The logs show that all clients after visiting were redirected to new foreign website with the script they downloaded and executed |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The helpdesk of yummyrecipesforme was flooded by customer's emails who declared after visiting the website, the website pushes a file to download, all costumers downloaded and executed that file thinking it was free recipes. Notice after executing that this file was redirected to a new website called greatrecipesforme and their computers now work slow.  Using a sandbox client repeating the same steps and using tpcdump for inspection all connections done it, identifying the greatrecipesforme´s IP besides we notice all connections to this foreign website receive more information than should, excluding the TCP handshake. All clients and internal webmaster, their credentials were changed. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Recommendation actions are implementing:   * Multi Factor Authentication: adding this method, the attempts of change passwords from malicious actors, verifying the owner of the account really try to change his password. * Password policies: use password policies to avoid the robbing of credentials using brute force, avoid using previous passwords and remember changing password every 90 days |