# Cybersecurity Incident Report

|  |
| --- |
| **Session 1: Identify the network protocol involved in the incident** |
| After a change in the source code of the site *yummyrecipesforme.com* a javascript code was added, which using the **HTTP : GET** method through the **HTTP** protocol, asks visitors to download a malicious file, which after execution redirects them to another URL address of a clone site. |
|

|  |
| --- |
| **Session 2: Document the incident** |
| Several customers of the *yummyrecipesforme.com* website contacted the company's technical support informing that when accessing their site, they were asked to download a file that would supposedly update their browsers, then reported being redirected to another similar site, but with a different address and with the same products offered on the original site being made available for free, in addition, their computers have been operating slowly since then. In response, the owner tried to access the site's admin panel but was unsuccessful, so he contacted our company to investigate the incident.  A sandbox environment was created for the investigation, the **tcpdump** tool was used to create a DNS & HTTP traffic log to analyze the network when accessing the site. As soon as the loading of the site is completed, a request to download an executable appears, claiming the purpose of updating the browser, after downloading and allowing it to run, the browser redirects the page to another URL address *greatrecipesforme.com* which has an identical interface to the previous one, however, with the products sold on the original site being offered for free.  The analysis of the log file of this operation shows that after a connection has been established between the source computer and the destination site *yummyrecipesforme.com*, already at the application layer the browser requests data from the site using the **HTTP : GET** methodthrough the **HTTP** protocol, which initiates the download of the malicious file, which then redirects the user to the clone site.  A senior analyst confirmed the compromise of the original site, which occurred through a change in its source code, with the addition of a javascript code that makes the request for the malicious download to the visitor, and the analysis of the downloaded file found the script that makes this redirect.  It was later discovered that the password of the administrator account was still set as the default password and there was also no type of control such as two-factor authentication, these facts together with the change of the credentials of the administrator account are strong indications that the attacker possibly already had knowledge of the login and password of this account or used a brute force attack to gain access. |

|  |
| --- |
| **Session 3: Recommend a remediation for brute force attacks** |
| An essential security measure that is recommended, and that can prevent any of the hypotheses of compromise raised from occurring, is two-factor authentication, because in addition to the login and password credentials, it requires that whoever is trying to gain access to the account verify its authenticity through another means, such as biometric data or a one-time password sent by email or phone.  Two other recommended measures include stricter password creation policies, i.e. passwords that do not include dates or obvious sequences of letters or numbers, and also limiting the number of login attempts. |