Security incident report

Section 1: Identify the network protocol involved in the incident

HTTP protocol

Section 2: Document the incident

After users complained that yummyrecipesforme.com requested them to download a file and run it on their machines, that the URL of the site has changed and that the site is too slow, the site owner tried to login to the web server but it was blocked.

Using a sandbox an analysis was done and the log file shows that after a successful DNS resolution request, after the connection to the site **yummyrecipesforme.com** established through the HTTP protocol, was asked to download the file.

After running the file there was a new request for DNS resolution, this time to the IP address of the site **greatrecipesforme.com** that looked identical to the original site (**yummyrecipesforme.com**).

The senior of the Cybersecurity team analyzed the source code of the site and the download file, he found that the attacker manipulated the website (to enter the file to users) and as the site owner could not login, he believes that a brute force attack occurred and then the password was changed. When a user runs the file on his computer, he compromises it.

Section 3: Recommend one remediation for brute force attacks

One of the best and simplest ways to prevent a brute force attack is by using 2-factor authentication, where you first identify yourself by putting your password, and then you need to confirm that you are you, through a code that can be sent to you or generated in some application.