# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocol involved is the Hypertext transfer protocol (HTTP). We used tcpdump to access the company’s official website (yummyrecipesforme.com) to analyze the problem through seeing the DNS and HTTP traffic logs that were recorded during the tests of the incident. These tests provided proof of our conclusion. The malicious file sent to the clients’ computers from the threat actor was done by utilizing the HTTP protocol at the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| We initially found out about the incident through customers reaching out to us stating that after visiting the company’s website, a file was downloaded to their computer causing their computer to slow down drastically. The website owner was also consequently locked out of their own account after trying to connect to the website.  A sandbox environment was used to test the website without doing harm to the company network. We then ran tcpdump to get a log of traffic information after testing the website through our own interactions with it. We were then prompted to download a file after visiting the website claiming to update the browser which caused us to get redirected to an identical fake website (greatrecipesforme.com) displaying the company’s secret recipes. The file downloaded was malicious software.  After analyzing the tcpdump log we came to the conclusion that the process was the following:   * The IP was requested, and once the connection was established over the HTTP protocol, the analyst recalled downloading and executing the file. * The logs then stated a new IP resolution for the greatrecipesforme.com URL. * Senior analysts concluded that the source code was manipulated by a threat actor to cause this malicious file to be downloaded and then redirect the client to the fake website revealing confidential company information. * Since the owner was locked out of their own account, the conclusion was made that a brute force attack where the threat actor guessed the password to the account to access it was the cause. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| One recommended remediation for the brute force attacks would be enabling two factor authentication on the owner’s account. This allows an extra layer of authentication protecting the owner from being a victim to someone trying to access their account. This is done by adding another personal source of communication from the owner like a phone number or separate email to confirm any login attempt made to the owner's company account. |