# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved is HTTP. Utilizing tcpdump to access the website yummyreceipesforme.com, the malicious file is shown to be transported to the user’s computer using the HTTP protocol. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Many customers reported the incident, stating that when visiting the website they were promoted to download and run a file which asked them to update their browsers, their computers have been working slowly ever since. The webpage owner noticed they were locked out of their account and contacted the website hosting provider.  The analyst used a sandbox environment to test the website, running tcpdump to capture the network and protocol traffic packets. The analyst confirmed what the customers were experiencing, updating the browser and then being redirected to a fake website greatreceipesforme.com that looked identical to the original site.  The browser initially requested for the IP address for the yummyrecipesforme.com website. After downloading the file, the network traffic changed requesting a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatreceipeforme.com website.  The team believes the attacker used a brute force attack to access the account and change the admin password. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One recommendation for brute force attacks is utilizing Two-Factor authentication. The password may have been a default one, but with 2FA, access would have only been permitted to the appropriate party, validating the correct identity. A brute force attack won’t be successful as it requires an additional authorization. |