# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| From looking at the tcpdump that was done we could see from the lines that the main target seemed to be an HTTP protocol on the yummyrecipesforme.com website. You can see the malicious file being sent to that specific target & ultimately affecting the DNS. | |
|

| **Section 2: Document the incident** |
| --- |
| After receiving initial reports from many customers our team decided to take a look and see what the users were experiencing. Upon investigation we noticed how users were being prompted to download a piece of software from the site and it was only then did their machines start to act slower for no explained reason. Once this was discovered our next course of action was to try and mimic this without harming our network, so once we had loaded up the website in a virtual machine and then proceeded to download the software. After this was done we then tried to access our server only to find out that we were locked out of it, this is when we escalated our problem to senior analysts.  The senior analysts took what we had downloaded in the virtual machine & inspected it fully to see what and how it was doing malicious activities. From there they noticed how the file was changing the IP and routing individuals to an alternate website (greatrecipesforme.com), deeper into the reading of the source code it was found the attacker had placed code within the base website that would trigger all of these events. With this knowledge and being locked out of the administrator account they determined it was a brute force attack. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Of the many security measures that can be implemented it is strongly suggested that two-factor authentication (2FA) are enabled with any and all accounts to help make an attack like this more difficult. It will also help and synergize with sending whoever is attempting to login a one-time password (OTP) to the specified device. With these security choices it should greatly stop any attack that can be considered brute force. |