# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The protocols involved in the incident were HTTP and DNS | |
|

| **Section 2: Document the incident** |
| --- |
| The incident occurred at 14:18. The tcpdump logs show the following; The browser initiated a DNS request, looking for the IP of the yummyrecipesforme.com URL. The DNS replied with the correct IP address,  The browser initiated an HTTP request looking for a webpage using the IP address sent by the DNS. The browser then downloads the malware, and initiates another DNS request to find the IP of the greatrecipesforme.com URL.  Finally the browser initiates another HTTP request to the IP returned. After looking at the malware file the analysis concluded that it contained a script to redirect visitors from yummyrecipesforme.com to greatrecipesforme.com. It was also concluded that the web server was impacted by a brute force attack. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| A recommendation would be to limit the number of login attempts. This would reduce brute force attacks from occurring, in addition to this a MFA should also be implemented in case the threat actor already knows the password. |