# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The port this incident took place on was Port 80. Commonly used for HTTP connections between the source PCs and the destination Server. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Initially, the incident was first documented at 14:18. A previous DNS resolution request was successful, allowing us to access the site. When on the site, a piece of malware was hiding behind an unauthorized ‘Get Free Recipes ‘button. This is evidenced by the ‘HTTP GET’ method using HTTP protocol 1.1. This indicates a file download, which is believed to be a malicious file. We believe the threat actor gained access to the server by way of brute forcing the administrator password(s). They were then able to redirect user web traffic onto another webserver. We see this by way of another DNS resolution request taking place at 14:18 at the same time we first visited our website, redirecting web traffic to  greatrecipesforme.com. The malicious code that was downloaded onto user’s machines by means of promising them free recipes is now slowing down infected PCs. This attack indicates social engineering by promising people free recipes once the unauthorized button is clicked, as mentioned above, their traffic is redirected, and the malicious code is downloaded onto their PCs. Complaints stem from the affected PC’s slowing down which may indicate that the code is designed to consume too many resources on the affected PCs that could ultimately lead to system crashes. As a side note, it is apparent that the threat actor has changed the admin password, thus locking authorized users out of the admin console. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| The immediate remediation relies on being able to regain access of the admin account. Once that is rectified a new password policy would need to be implemented for business-critical infrastructure, like the webserver and admin account. I would also recommend a multi factor authentication method for this, as an added layer of security. |