# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Users emailed the help desk stating that the site yummyrecipesforme.com is asking them to download a file after loading the web page via HTTP. After downloading the file the users were redirected to the site greatrecipesforme.com, which contains the malware. DNS redirect was created. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| 1. Customers going to the yummyrecipesforme.com were asked to download a file that caused their computers to run slow and redirects the browser to greatrecipesforme.com, which contains the malware. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| 1. change the current password for the admin panel.  2. create a policy to change critical passwords for after a specific period of time (6 months as an example)  3. isolate the admin panel from the DMZ. |