# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The DNS protocol is involved in the incident. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A former employee accesses the admin panel and decides to lure users to a fake websites with malware, when users type the yummyrecipesforme.com website their browsers prompt to download a file with malware. The website owner cannot access the admin panel because the former employee changed it, Typically the browser initiates a DNS request and requests the IP Address of the yummyrecipesforme.com URL from the DNS server, the DNS replies with the correct IP address, then an HTTP request to request the webpage from yummyrecipesforme.com using the IP Address sent by the DNS server, when the malware is prompted to download a sudden change in logs occur and the traffic is routed to another website greatrecipesforme.com which most likely contains the file with malware. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Stronger password policies, passwords should be changed in the event an employee resigns or the admin panel should only be accessed by authorized users. |