Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocols involved in this incident include Enterprise Virtual Private Networks in respects of the company website, IPSEC which is commonly used in site-to-site VPNs to create an encrypted tunnel between the primary network and the remote network. The problem with site-to-site VPNs is how complex they can be to configure and manage compared to remote VPNs which is most likely how the threat actors were able to re-route the website from the correct company website to the fake website. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A disgruntled baker affiliated with the compromised company website decided to disrupt the company website and re-route the server to a fake dummy website where its best selling recipes are posted for free. Customers are reporting that on the website, you are prompted to download a file which has caused slower operations of their computer devices resulting from being on the company website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Multi-factor Authentication (MFA) and two factor authentication (2FA) due to the extensive identity verification ensuring more complications for a potential future event to arise. |