# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol involved in this incident was HTTP. The network analyzer tool tcpdump listed the DNS and HTTP logs which were involved in the communication between the users , servers and the attacker devices. The protocol HTTP works in the application layer because of which the browser downloaded the malicious file into the user’s device, |
|

|  |
| --- |
| **Section 2: Document the incident** |
| **The Scenario**  The users of yummyrecipesforme.com tried to access the website but their browser prompted them to download an executable file which after running redirected them to a different website named greatrecipesforme.com whose design looked exactly like the original website but the recipes that the company sold were now available for free. The users also reported that their devices now began to run slowly.  **Technical details**   1. The browser requests a DNS resolution of the yummyrecipesforme.com URL. 2. The DNS replies with the correct IP address. 3. The browser initiates an HTTP request for the webpage. 4. The browser initiates the download of the malware. 5. The browser requests another DNS resolution for greatrecipesforme.com. 6. The DNS server responds with the new IP address. 7. The browser initiates an HTTP request to the new IP address. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| * Since the emergence of brute force attack has made even the strongest passwords guessable, Multi factor authentication should be implemented as getting through it is no longer just about cracking the right set of characters. |