# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The Hyper Text Transfer protocol (HTTP) is used to send request to web servers for web pages and also in this case it is used to download an unknown malware into customers computer by an attacker using the HTTP protocol | |
|

| **Section 2: Document the incident** |
| --- |
| Several customers contacted the website’s helpdesk stating that when they  visited the website, they were prompted to download and run a file that  contained access to new recipes. Their personal computers have been  operating slowly ever since and the website address was also changed.The website owner tried logging into their account but is locked out.  The Cybersecurity analyst accessed the website in a sandbox environment and ran tcpdump to capture network traffic logs. As mentioned by customers, the analyst was prompted to download a file saying it provides access free recipes then downloaded and ran it which redirected the browser to a fake website.  The tcpdump logs state that after downloading and running the file, the browser initiates a DNS request to new IP address and the connection to that new IP address is formed.  Upon analyzing the downloaded file it consist of a piece of code that prompts user to download a malicious file which is done by the attacker using the website owner admin account after using brute force approach to change the password. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To prevent these approaches in the future, frequent password updates is required making sure that no old passwords are repeated so that even if an attacker knows the previous password they can’t use it and security hardening is essential , mainly network hardening practices like using MFA- Multi factor authentication which decreases the chances of brute force approach or 2FA- Two - factor authentication which after entering password sends otp to their phone or email for a limited time which makes the brute force approach impossible. |