# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Network protocol involved in the incident is the HyperText Transfer Protocol (HTTP) protocol. Running tcpdump and analyzing the logs have provided evidence that supported this conclusion. The malicious file is observed being transported to the users computers using the HTTP protocol at the application layer. | |
|

| **Section 2: Document the incident** |
| --- |
| Multiple customers reached out to the help desk saying that the company’s website had prompted them to download a file, which made their system slow. To analyze this incident, a sandbox environment was created and started a network protocol analyzer and tried to access the website. Initial connection is fine, then the analyst is prompted to download a file saying that it would update the browser, accepts the prompt and runs it, then the browser requests another DNS resolution for a spoofed website and connection is established to the fake website.  The senior analyst analyzed the source code for the websites and the downloaded file. The analyst concluded that an attacker had manipulated the source code that prompted the users to download a malicious file as a browser update. Since the website has been locked out of their administrator’s account and changed the admin password, the team believes that it must be a brute force attack. The execution of this malicious file compromised the users systems. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| 1. The changing of password from the default to a more secure password. 2. Monitoring login attempts and limiting them and implementing CAPTCHA service. 3. Implement MFA or 2FA. |