Security incident report

Section 1: Identify the network protocol involved in the incident
The internet protocol involved in the incident was Hypertext Transfer Protocol (HTTP). To verify the cause of the incident, the IT team created a Sandbox environment to replicate the problem reported by the customers.

Section 2: Document the incident
Several customers visiting the companies website expressed that when the website was uploaded they were prompted to download a file. The file redirected the customers to another similar website. The owner of the company tries to login into the admin panel but was not able to login. The cybersecurity analyst created a sandbox environment to protect the company's website from further harm. While in the sandbox environment the analyst deployed a TCPdump and uploaded the website and was prompted to download the file. Once the file was downloaded, the website name changed to another name which presented a fake version of the original website. A senior analyst confirmed that the website was compromised. The analyst noticed that a javascript code had been added to prompt visitors to download the file. Which in turn redirected from the original website to the fake website. The analyst discovered that the attacker used a brute force attack to get inside the admin account and changed the password and locked the owner out.

Section 3: Recommend one remediation for brute force attacks
One security measure we recommend is Multi-factor authentication (MFA).

This will protect against brute force attacks by having another layer of verification before gaining access. While having this implemented if a threat actor happens to pass the first layer of security the threat actor still has to get passed another layer of security.