# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The protocol involved in the incident was HTTP. The browser initiates an HTTP request to the website using DNS and an application is downloaded to the user’s device. The device is redirected to the new HTTP domain by the downloaded application. | |
|

| **Section 2: Document the incident** |
| --- |
| Customers reported the application download and the problem of slowness of their computers after the download. They also reported the change in the domain name after the download.  The team began the investigation immediately. They contacted the host provider and found out they no longer have access to the administrative account. Next, they went through the process as the users described in a sandbox. They ran tcpdump to capture the traffic in the process of connecting the website, downloading, and redirecting to the fake website. The cybersecurity team experienced the issue as customers described. After loading the real website, they were prompted to download an application. After downloading the application, they were redirected to the fake website. The logs on the tcpdump show the exact same process.  By analyzing the source code of the real website, they found the manipulated code in their javascript code that prompted users to download a software. As they are locked out of their administrative account, it can be deducted that their password has been compromised. This can be either through a brute force attack, or someone with access to the password accidentally gave it out. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| It is recommended to have a 2-factor authentication for entering the administrative account. This can be through one-time passwords or a biometric of the owner. Also, it is recommended to put a maximum number of trials on the password per IP address. Another way to avoid this type of attack is to use more complex and longer passwords, which take a lot longer and the cybersecurity team has more time to get notified about the attack, before it happens. |