# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Hypertext Transfer Protocol (HTTP) is involved in the incident.  The browser sends a DNS request to the server to get the IP address of the domain “yummyrecipesforme.com”, after the connection is successful, the website downloads an exe file for the user. When the file is running, the device will be infected by a malicious code that will redirect the webpage for “yummyrecipesforme.com” to “greatrecipesforme.com” that contains another malware. | |
|

| **Section 2: Document the incident** |
| --- |
| Multiple customers emailed yummyrecipesforme’s helpdesk and complained that the website had prompted them to download a file to access free recipes. After running the file, the address of the website changed and their personal computers began running more slowly.  In response, the website owner tries to log in to the admin panel but is unsuccessful, so they reach out to the website hosting provider. The response team is tasked with investigating this security event.  Because the owner of the website cannot access it using his administrator credentials, we believed that a malicious actor had executed a brute force attack at the web page and the website was compromised. The actor gained an administrative account and injected a malicious code to the website to prompt users to download the malicious file.  To address the incident, the response team used a sandbox environment to simulate the suspicious behavior of the website. The team used a network protocol analyzer, tcpdump, to check the logs. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| The brute force attack was successful because the admin password was still set to the default password. A recommendation to avoid brute force attacks is to implement Password Policies and frequent password updates within the organization. Another recommendation would be the use of Multi factor Authentication(MFA) or two-factor authentication(2FA). |