# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The incident involved the DNS and HTTP network protocols, which are essential for communication and resolution of IP addresses associated with accessed domains. The DNS protocol was used to resolve the IP address of both websites involved in the incident: yummyrecipesforme.com and the fake website greatrecipesforme.com. After resolving the IP address of the legitimate website, the HTTP protocol was employed to load the web page content. This content included a malicious script that redirected users to the malicious website via a new DNS request, resulting in a download of disguised malware claiming to provide access to free recipes. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| After a successful brute force attack, the former employee gained access to the website’s admin panel. The attacker exploited a vulnerability in a still-active default password and, without additional protection against excessive login attempts, was able to access the admin account. Once in control of the panel, the attacker inserted malicious JavaScript code into the source code of the yummyrecipesforme.com website. This code prompts visitors to download a file claiming it would provide access to free recipes. Upon download, users are redirected to greatrecipesforme.com, a fake version of the website containing the malware.  Following the incident, customers reported performance issues on their devices and received unusual messages asking them to download files. When the website owner attempted to access the admin panel to investigate, he found that the password had been changed, blocking access. Further analysis confirmed that the website had been compromised and the malicious code was active. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To prevent brute force attacks in the future, the following security measures are recommended:  1. Implement Multi-Factor Authentication (MFA): Add MFA for all administrative accounts, requiring a second authentication factor in addition to the password.  2. Strong Password Policy: Ensure that all administrative account passwords adhere to security best practices, requiring a combination of special characters, numbers, and a minimum length of 12 characters. Avoid default passwords and disable accounts with default credentials.  3. Limit Login Attempts and Temporary Lockout: Configure the system to temporarily lock the account after a specific number of failed attempts, making brute force attacks more difficult.  4. Security Monitoring and Alerts: Implement monitoring systems that send alerts when unusual activity is detected, such as multiple failed login attempts in a short period of time.  5. Disallow the use of old passwords: Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it is important to prevent old passwords, such as default passwords, from being used to reset the password.disallow the use of old passwords. Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it is important to prevent old passwords, such as default passwords, from being used to reset the password. |