# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| During the analysis using **tcpdump**, several key network protocols were identified across different layers of the TCP/IP model:   * **DNS (Domain Name System)** – Application Layer  Used to resolve yummyrecipesforme.com and greatrecipesforme.com to their respective IP addresses. * **HTTP (Hypertext Transfer Protocol)** – Application Layer  Used for the initial web request and to download the malicious file. * **TCP (Transmission Control Protocol)** – Transport Layer  Ensures reliable delivery of data between the browser and the web servers. * **IP (Internet Protocol)** – Internet Layer  Routes data packets between hosts.   These protocols confirm standard web browsing activity layered with malicious redirection and executable download. | |
|

| **Section 2: Document the incident** |
| --- |
| The website yummyrecipesforme.com, which sells digital recipes and cookbooks, was compromised through a **brute force attack**. A **former employee** executed this attack by attempting multiple default passwords for the admin account. Eventually, the correct password was guessed, and the attacker gained unauthorized access to the website’s administrative panel.  Once logged in, the attacker embedded **malicious JavaScript** into the website’s source code. This script triggered an automatic prompt for visitors to download an **executable file** disguised as a browser update. Upon downloading and running the file, users were redirected to a **malicious clone website**, greatrecipesforme.com, which contained embedded malware. Users also experienced performance degradation on their personal devices.  **Discovery**:  The incident was reported after multiple customers emailed the helpdesk, stating they were prompted to download files and experienced browser redirection and slow computer performance.  **Investigation Details**:  The cybersecurity team, using **tcpdump** in a sandbox environment, observed the following:   * A **DNS request** to resolve yummyrecipesforme.com * An **HTTP request** to download the executable * A subsequent **DNS request** for greatrecipesforme.com * An **HTTP redirect** to the malicious site   The team also reviewed the website's source code and found the JavaScript redirection and download logic embedded by the attacker. Analysis of the executable file confirmed it contained redirection instructions and malware.  **Root Cause**:  The admin account used a **default password**, and there were **no security controls** (e.g., login throttling or 2FA) to prevent or detect the brute force attack. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To prevent future brute force attacks, it is recommended to **limit the number of login attempts** on all administrative interfaces.  **Why This Works**:  Brute force attacks rely on attempting many passwords in a short period. By limiting login attempts to a maximum of, for example, **5 per IP address**, and then enforcing a **temporary lockout or CAPTCHA**, you severely hinder the attacker’s ability to guess passwords rapidly. This also creates alert points for monitoring suspicious activity.  This control, combined with using **strong passwords** and **multi-factor authentication**, significantly reduces the likelihood of successful brute force intrusions. |