# Incident Analysis

## Log and Report Analysis

Our analysis of the tcpdump logs revealed a concerning sequence of events: users initially accessed (link unavailable) but were suddenly redirected to (link unavailable) due to injected malicious code. The attacker likely gained unauthorized access to the administrator account, modifying the password and locking out the owner. The incident report mentioned that users were prompted to download a disguised browser update, which was malware, compromising their computers.

## Recommended Actions

Our analysis suggests that the incident was likely rooted in a compromised administrative password. To prevent similar incidents and enhance security, we strongly recommend the following measures:

1. Implement a Detection System for Suspected Brute Force Attacks: Installing a robust detection system will enable swift identification and response to brute force attacks, minimizing potential damage.
2. Implement Multi-Factor Authentication: Enhance account security by requiring users to provide multiple forms of verification, significantly reducing the risk of unauthorized access.