# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The primary network protocol identified in the tcpdump captures is **HTTP over TCP**. The logs show a sequence of DNS requests and responses that resolve domain names (e.g., yummyrecipesforme.com and greatrecipesforme.com), followed by HTTP traffic specifically, the HTTP GET requests used to retrieve the website’s main page and the malicious payload. This indicates that HTTP is the protocol used for both normal web browsing and the subsequent redirection to the spoofed website. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| During the investigation of the security event for yummyrecipesforme.com, it was determined that the website was compromised by a former employee acting as a malicious insider. The attacker conducted a brute force attack on the admin panel by repeatedly attempting several known default passwords until gaining access. Once inside, the attacker modified the website’s source code by embedding a JavaScript function designed to prompt visitors to download an executable file. When customers visited the website, their browsers were forced to download this file. After execution, the file redirected users from yummyrecipesforme.com to a spoofed domain, greatrecipesforme.com, where malware was subsequently delivered.  The tcpdump logs confirmed the sequence of events:   * A DNS request is sent by the user’s machine to resolve yummyrecipesforme.com, followed by a correct DNS reply with the website’s IP address. * The browser initiates a TCP connection and an HTTP GET request to load the webpage. * Shortly after, another DNS request resolves greatrecipesforme.com, and an HTTP connection is established with the spoofed site.   These events correlate with customer reports of unexpected download prompts, redirection to an unfamiliar website, and degraded system performance. The evidence indicates that weak administrative password policies and a lack of controls to prevent brute force attempts allowed unauthorized access to the web host, leading to the website’s compromise and the delivery of malicious content. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To prevent similar brute force attacks in the future, it is recommended to **implement multi-factor authentication (MFA) for administrative accounts**. This security measure is effective because:   * It requires attackers to provide an additional verification factor (e.g., a code from a mobile device) beyond just a password. * Even if an attacker successfully guesses or otherwise compromises the password, they would still be blocked from accessing the system without the second factor. * MFA significantly reduces the risk of unauthorized access due to brute force attempts, as it adds an extra layer of defense that is not solely reliant on password strength.   Implementing MFA, combined with enforcing strong, non-default passwords and monitoring login attempts for suspicious activity, will provide a robust defense against brute force attacks and help secure the website against future intrusions. |