Tcpdump-Security-Incident-Report

Security Incident Report

1. Network Protocol Identified

Based on the tcpdump log, the two primary network protocols involved in this incident are:

- DNS (Domain Name System) – used to resolve the domain names yummyrecipesforme.com and greatrecipesforme.com to IP addresses.
- HTTP (Hypertext Transfer Protocol) – used to request and deliver the web pages, including the malicious download and redirect activity.

- Incident Summary

Customers visiting yummyrecipesforme.com experienced unexpected prompts to download a file. The issue was reported after multiple users contacted support, stating that the website prompted them to download a file to access free recipes. After running the file, their browsers redirected to greatrecipesforme.com, and their systems began running slowly.

A security investigation was launched. A tcpdump capture revealed the following:

- A DNS request was made for yummyrecipesforme.com, followed by an HTTP GET request to load the main page.
- The browser then initiated a file download, triggered by malicious JavaScript embedded in the website’s source code.
- A second DNS request was made for greatrecipesforme.com, and an HTTP connection was established to that domain.
- These steps confirmed a redirect via malware.

Further review by the cybersecurity team and a senior analyst showed that the website source code was modified. JavaScript was injected to prompt file downloads. The attacker used a brute force attack to gain access to the admin panel, exploiting the use of a default admin password. After gaining access, they updated the site code and locked out the original admin by changing the credentials.

Sources of information:

- tcpdump network traffic log
- Customer support tickets
- Admin access failure report
- Manual code inspection by a senior analyst

3. Recommendation to Prevent Brute Force Attacks

To prevent future brute force attacks, it is recommended to enforce multi-factor authentication (MFA) for all administrative logins.

Why it's effective:
MFA requires users to verify their identity with more than just a password—such as a code sent to a phone or email, or a biometric factor like a fingerprint. Even if an attacker guesses or obtains the password, they will not be able to access the account without the second authentication factor. This adds a strong layer of protection against brute force and credential-based attacks.