TCPdump traffic Report

Summary:

The connection between your computer and **yummyrecipesforme.com** was successful from **14:18:32 to 14:18:36**, and no issues were observed during this period. The incident begins at **14:25:29**, when the **TCP handshake** reaches its third step. During this phase, the server **greatrecipesforme.com (port 80)** responds with a **SYN-ACK** and a **Push ACK**, completing the handshake with your machine.

However, at **14:25:29.576597**, an unusual event occurs. Instead of your computer initiating further communication, the server (**greatrecipesforme.com**) tries to establish a connection to your machine on port **56378**. This unexpected behavior suggests that **malware** may have been installed during the **Push ACK** phase, especially since the connection used HTTP **1.1**. This could indicate a potential **malicious activity**, possibly involving **data exfiltration** or unauthorized access.

Recommendation:

To enhance security and protect against potential malware infections, it is strongly recommended to implement **Two-Factor Authentication (2FA)** for any web application or service that requires user credentials. **2FA** adds an extra layer of protection by requiring a second form of authentication, such as a temporary code from an authentication app or an SMS message, in addition to the usual password.

By requiring **2FA**, even if a malicious actor manages to steal or guess the password, they would still need the second factor to access the account. This makes it significantly more difficult for attackers to gain unauthorized access, reducing the risk of sensitive data exposure and protecting against attacks such as **credential stuffing**, **phishing**, and **data breaches**.