Section1:

Per the TCP dump the only network protocols being used are the DNS and HTTP protocols.

Section 2:

Based on the log data we can see that following a DNS connection to the proper website “yuummyrecipiesforme.com” some volume of normal http data was transferred from the server to the connection. After a period of seemingly normal execution a new DNS request was started that was not initiated by the user, and this redirects the user to “greatrecipiesforme.com”. Now more http activity occurs not on the proper website.

Section 3:

Using this information to conclude the website has been compromised through brute force we can secure against this method of attack through 2FA requiring users to confirm a login through an allowed secure device.