Security incident report

Section 1: Identify the network protocol involved in the incident
This incident happened over HTTP(Hyprtext transfer protocol). After running tcpdump while connecting to yummyrecipesforme.com it was observed that the malicious file was being transferred to users computers via HTTP.

Section 2: Document the incident
Yummyrecipeforme.com customers have been reaching out to the helpdesk, stating that when visiting the website, they are prompted to download and install a file when they first get to the domain. It was reported that after they downloaded and installed the malicious file, they began experiencing their computers being slowed down and that the website would redirect to a different URL. The website owner was unable to login after being notified. The security team started a sandbox environment to investigate and diagnose the issue. After loading into the sandbox, we used tcpdump and connected to the website as to not damage company networks. Upon visiting yummyrecipesforme.com, we were directed to download and install the file under the guise of free recipes. The browser was then redirected to (greatrecipesfome.com). After inspecting the tcpdump log, it was observed that the browser initially requested the proper IP address. The connection was made over HTTP we downloaded and ran the file. It was observed that after execution the browser redirected to (greatrecipesforme.com) and showed an increase in traffic. After handing over the information to the senior analyst, he was able to determine that a malicious actor has manipulated the code of the site to prompt users to download the malicious file disguised as a browser update. The fact that the website owner was locked out of his account leads the team to believe that this may have been a brute force attack to access the owners

account and change the password. The malicious file compromised end user's devices.

Section 3: Recommend one remediation for brute force attacks
It is recommended that all users start using MFA(Multi-Factor Authentication) to secure their account. This incident was caused by a malicious actor being able to guy a password from having previously worked with the website owner. It is advised to use MFA as a second form of authentication because it allows users a second layer of defense by having to authenticate that it is the owner of the account logging in every time.