Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident
The protocol affected in the incident is Hypertext Transfer Protocol (HTTP). By running tcpdump and accessing the yummyrecipesforme.com website, we were able to detect the issue and capture protocol and traffic activity in a DNS & HTTP traffic log file, which provided the evidence necessary to reach this conclusion. The analysis revealed that the malicious file was being delivered to users' computers via the HTTP protocol at the application layer.

Section 2: Document the incident
Multiple customers reported to the website owner that upon visiting the site, they encountered prompts to download and execute a file, purportedly for browser updates. Subsequently, their personal computers experienced diminished performance. Upon attempting to log into the web server, the website owner discovered being locked out of their account. A cybersecurity analyst employed a sandbox environment to assess the website's behavior without affecting the company network. By utilizing tcpdump, the analyst captured network and protocol traffic packets generated through interactions with the website. Upon accepting and executing a file claiming to update the browser, the analyst found themselves redirected to a counterfeit website (greatrecipesforme.com) closely resembling the original site (yummyrecipesforme.com). Examining the tcpdump logs, the analyst noted the browser's initial request for the IP address of yummyrecipesforme.com. Following the establishment of a connection via the HTTP protocol, the analyst recalled downloading and running the file, leading to a sudden shift in network traffic as the browser sought a new IP resolution for greatrecipesforme.com. Subsequently, the traffic redirected to the new IP address associated with the counterfeit website. A senior cybersecurity professional scrutinized the source code of both websites and the downloaded file. It was determined that an attacker had

tampered with the website, embedding code to prompt users to download a malicious file disguised as a browser update. Considering the website owner's report of being locked out of their administrator account, the team surmised that the attacker likely employed a brute force attack to gain access and alter the admin password. As a result, the execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
To fortify defenses against brute force attacks, the team intends to deploy two-factor authentication (2FA). This 2FA strategy will mandate users to verify their identity by authenticating a one-time password (OTP) dispatched to either their email or phone. Upon confirmation of both their login credentials and the OTP, users will be granted access to the system. This additional layer of authorization significantly mitigates the likelihood of malicious actors succeeding in brute force attacks, as it necessitates supplementary validation beyond standard login credentials.