Kimberly Chau

Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). As the web server for yummyrecipesforme.com could not be reached, it shows HTTP is involved since it deals with requests to web servers for web pages. Based on the tcpdump traffic log, we see that the HTTP:GET method is used to request data from yummyrecipesforme.com at the application layer, which is a sign for the download request for the malicious file.

Section 2: Document the incident
Multiple customers reported that the company's website prompted them to download a file to access free recipes and then, after running the file, the address of the website changed and their personal devices began running more slowly. The website owner attempted to log in to the admin panel but failed. To observe the website behavior, our group of cybersecurity analysts created a sandbox environment and ran tcpdump while opening yummyrecipesforme.com. Once the website is loaded, we're prompted to download an executable file to gain access to free recipes. After accepting the download and running the file, the browser redirected us to greatrecipiesforme.com, which contained malware. After further inspection with the tcpdump logs, we noticed the browser initially requests the correct IP address of yummyrecipesforme.com. But once a connection is made with the website over the HTTP protocol, the browser prompts a download and after running, requests the IP address of a different, fake website, greatrecipesforme.com. A senior analyst checked the source code for the website and found that javascript code had been added to prompt website visitors to download a file and redirect them to a different website. The cybersecurity team reported the web server was impacted by a brute force attack by a former employee.

Section 3: Recommend one remediation for brute force attacks
One remediation for brute force attacks we can implement is requiring more frequent password changes since the former employee was able to successfully make the brute force attack due to the admin password still being set to the default password. This would help prevent future attack since it would be hard for an attacker to guess a password that is changed often.