Security incident report

Section 1: Identify the network protocol involved in the incident

The protocol impacted in attack is HTTP in the application layer. By using network protocol analyzer tcpdump, we found that the malware file is being transported to users computer through HTTP protocol.

Section 2: Document the incident

Several customers contacted website helpdesk and complained that the company's website has prompted them to download some file to update their browser, and after running the file, address of the website changed and their computers are running slow

The security analysts responded by creating a sandbox environment to observe the suspicious website behavior. After running tcpdump and running website yummyrecipesforme.com , as soon as website loads , we are asked to download a file to update the browser. When we run the file,we are redirected to another address or website greatrecipesforme.com ,that looks like the original website and contains the recipes for free that yummyrecipesforme.com sells.

The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website.

It is high possibility that the website is under brute force attack where some disgruntled baker has executed attack by guessing password of administrative account . After obtaining the login credentials, they embedded a javascript code in source code that prompts visitor to download a file and redirects the browser to other website.

Section 3: Recommend one remediation for brute force attacks

Implementation of 2FA will surely mitigate risk of brute force.