SECURITY INCIDENT REPORT

Section 1: Identify the network protocol involved in the incident

The protocol impacted in the incident is Hypertext transfer protocol (HTTP). Running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log.

Section 2: Document the incident

Several customers contacted the website owner stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account.

We used a sandbox environment to test the website without impacting the company network. Then, we ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. It was prompted to download a file claiming it would update the user's browser, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com).

Since the website owner stated that they had been locked out of their administrator account, the team believes the attacker used a brute force attack to access the account and change the admin password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks

Two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system.