Security incident report

Section 1: Identify the network protocol involved in the incident

The protocol impacted in the incident is Hypertext transfer protocol (HTTP).

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. After running the file, the address of the website changed and their personal computers began running more slowly. The website owner tries to log in to the admin panel but they were logged out.

The cybersecurity analyst used a sandbox environment to observe the suspicious website behavior. The Analyst then runs the network protocol analyzer tcpdump, then tries to hit the URL yummyrecipesforme.com. As soon as the website loads, it is then prompted to download an executable file to update your browser. The Analyst accepted the download and allowed the file to run . The browser then redirects you to a fake website (greatrecipesforme.com) which is designed to look like the original website (yummyrecipesforme.com).

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.

The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst discovered that an attacker had manipulated the website to add code that prompted the users to download a malicious file disguised as a browser update. 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

One security measure the team plans to implement to protect against brute Force attacks is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identity 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. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization.