Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is the Hypertext Transfer Protocol (HTTP) as part of the application layer of the TCP/IP model.

Section 2: Document the incident

This incident was discovered when several customers reported strange activity on the company website and the website owner was unable to login to their admin panel. The incident occurred when a former employee, now threat actor, compromised the web host with a successful brute force attack. The threat actor embedded a malicious JavaScript function into the website's source code as detailed by the log files collected in a sandbox environment and investigation of the website source code. Logs showed that when users successfully connected to the website a HTTP GET method request is used to request data from the website. This request is acknowledged, and a long wait appears to happen before a request is made to the DNS servers again for a different non-organization URL "greatrecipesforme.com" and on a different port. This long wait is further categorized by users reporting a loss in operating speed in their system, indicating increased load on the system commonly caused when downloading something. Once the IP is retrieved the port changes again and attempts to connect to this new malicious website which ends in success.

Section 3: Recommend one remediation for brute force attacks

A recommendation to help mitigate these attacks in the future is to implement a strong password policy followed by some form of MFA (Multi-factor authentication). This incident was originally caused because the threat actor was able to perform a basic brute force attack by guessing the admin password to gain access as the owner of the website. By enforcing strong password policies this would not have happened, with multi-factor authentication even with the password the threat actor would not have been able to so easily access the admin panel. Implementing one or both of these is highly recommended to not let this happen again and mitigate especially insider threats.