Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident was both DNS and HTTP. For DNS, the browser had to look for the domains by requesting the IP addresses during the incident. This included the original domain (yummyrecipesforme.com) and the malicious redirect domain (greatrecipesforme.com) HTTP protocol retrieved the webpage and the downloaded the executable file. The HTTP requests also included the redirection traffic that occurred after the malware executed.

Section 2: Document the incident
How the intrusion happened It happened that a former employee gained unauthorized access to the website's hosting environment by performing a brute-force attack against the administrative login. Because the account was still using a default password and there were no protections in place to limit repeated login attempts, the attacker was able to successfully guess the credentials and enter the admin dashboard. What did the attacker change? After gaining access, the attacker modified the website's source code by embedding a malicious JavaScript function. This script forced website visitors to download and run an executable file disguised as a browser update. Once executed, the file redirected users to a fake website (greatrecipesforme.com) that hosted additional malware. What thee customers had experienced After some hours, the customers reported that the website asked them to download a file to access free recipes. After running the file, users noticed that their browsers redirected to a different URL and their computers operated more slowly.

A sandbox was used to check the behavior while capturing traffic with tcpdump. The logs showed normal DNS and HTTP requests to the original domain followed by additional DNS and HTTP traffic to the fake domain. A senior analyst confirmed the code injection by reviewing the website's source files and identified embedded JavaScript. This information served as evidence of the compromise.

Section 3: Recommend one remediation for brute force attacks
Implementing a policy that requires frequent password changes for the administrative account