Security incident report

Section 1: Identify the network protocol involved in the incident
Hypertext tanfer protocol (HTTP)-Application layer.

Section 2: Document the incident
Multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. To address the incident, we create a sandbox environment to observe the suspicious website behavior. We run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, we are prompted to download an executable file to update our browser. We accept the download and allow the file to run. We then observe that our browser redirects us to a different URL, greatrecipesforme.com, which contains the malware. We observed that the browser requested for ip address for yummyrecipesforme.com and the DNS server sent back the ip address (203.0.113.22)to the browser and all of a sudden the logs showed a sudden change in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. We notice that javascript code had been added to prompt website visitors to download an executable file. Analysis

of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com.

The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled hacker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack.

Section 3: Recommend one remediation for brute force attacks
1. Multi Factor authentication 2. Stronger password policies 3. Monitor login attempts 4. Limit number of login attempts 5. Require one time password(OTP) 6. Password should be changed often after the resignation of any employee, and stop the reuse of default passwords