Security incident report

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A former employee has decided to lure users to a fake website with malware.

The former employee/ hacker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After embedding the malware, the hacker changed the password to the administrative account. When customers download the file, they are redirected to a fake version of the website that contains the malware.

Several hours after the attack, 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.

In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event.

To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which contains the malware.

The logs show the following process:

1. The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server.
4. The browser initiates the download of the malware.

5. The browser initiates a DNS request for greatrecipesforme.com.
6. The DNS server responds with the IP address for greatrecipesforme.com.
7. The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They 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.

Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

Section 1: Identify the network protocol involved in the incident
The network protocol involved in the incident is the HTTP protocol version 1:1 because the primary problem is accessing the yummyrecipesforme.com web server. Users are prompted to download the malicious file, which is sent to the visitors' computers using the HTTP protocol.

Section 2: Document the incident
• Multiple customers contacted the website's helpdesk, complaining that whenever they visited the website, they were asked to download and

run a file that would give them more recipes. Users complained that after downloading the file, their computers began running slowly.

- The website owner tried logging into the web server before realizing they had been locked out of their account.
- The cybersecurity analyst used a sandbox environment to open the affected website to avoid any impact on the company's network. The analyst then ran the tcpdump to monitor what network packets were interacting with the website.
- As users complained, the analyst was also redirected to the fake website “greatrecipesforme.com.”
- The cybersecurity analyst observed in the tcpdump log that the browser requested the IP address for yummyrecipesforme.com, but once the analyst downloaded and ran the file, a change in network traffic was evident as the browser began requesting the IP address for greatrecipesforme.com.
- The senior cybersecurity professional analyzed the source code for the websites and noticed that a former employee attempted a brute force attack to access the web host. The hacker tried multiple known default passwords until the right one was guessed.
- The login credentials obtained by the hacker were used to gain access to the admin panel and change the website's source code.
- The hacker embedded a javascript function in the source code that prompted users to download and run a file when they visited the website. When customers download the file, they are redirected to a fake version of the website that contains malware. The hacker then changed the password to the administrative account, ensuring that the admin was locked out.

Section 3: Recommend one remediation for brute force attacks
I recommend enforcing two-factor authentication (2FA) to avoid brute-force attacks. Two-factor authentication ensures that anyone who tries to log in as an admin needs to go through an extra step of verification apart from using their password before they get access to the web host. An OTP (one-time password) is a good way to enforce 2FA. This way, users are prompted to input a specific password sent by an automated client before accessing the web host. These OTP’s can be sent through text messages, emails, and authenticator applications.