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 HyperText Transfer Protocol was affected. In the tcpdump logs, it showed that there was a lot of traffic on port 80. Port 80 is used for HyperText Transfer Protocols. It also showed the HyperText Transfer Protocol downloading the malicious file to the users' devices when accessing the site. This indicates that the attacker likely exploited this network protocol during the incident.

Section 2: Document the incident
A former employee executed a brute force attack in order to gain access to the web host. When they obtained administrative access to the site, they

embedded a javascript function that prompted visitors to download a malicious file that redirected them to the fake version of the site containing the malware.

Some time after the attack, many customers contacted yummyrecipesforme's helpdesk. They stated that they were prompted to download a file to access free recipes on the site. When they ran the file, the site was changed and their computers also ran more slowly.

When the IT department heard about the incident, we created a sandbox environment in order to isolate and observe the suspicious website behavior. When we ran the network protocol analyzer tcpdump, the website prompted us to download an executable file, which had a script that redirected us to the malicious website, greatrecipesforme.com.

Section 3: Recommend one remediation for brute force attacks
We should apply a stronger password policy, or a multi-factor authentication in order to discourage brute force attacks. A stronger password policy will discourage the attacker from attempting the attack. A multi-factor authentication will be very helpful too since the attacker only obtained the password. They still cannot gain administrative access since they don't have any other way to prove themselves as trustworthy. In addition to that, we should change our administrative passwords more often so that the attacker cannot use dictionary attacks against us.