Security incident report

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A disgruntled baker has decided to publish the website's best-selling recipes for the public to access for free.

The baker 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 running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free.

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 update their browsers. 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 is designed to look like the original site. However, the recipes your company sells are now posted for free on the new website.

The logs show the following process:

1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request for the webpage.
4. The browser initiates the download of the malware.
5. The browser requests another DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

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 baker 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 protocols involved in the incident include DNS (Domain Name System) for domain resolution, HTTP (Hypertext Transfer Protocol) for website communication and file downloads, and potentially HTTPS (Hypertext Transfer Protocol Secure) for secure communication if the website used encryption.

Section 2: Document the incident
In this event, a individual successfully carried out a brute force attack on yummyrecipesforme.com, a website dedicated to the sale of recipes. By continuously attempting the administrative account's default passwords until the right one was guessed, the attacker was able to gain unauthorized access to the admin panel. Once logged in, the attacker altered the website's source code by inserting a malicious JavaScript function. For unaware visitors, this function caused the download and

execution of a file. The paid recipes were made available for free on a fake version of the website, greatrecipesforme.com, once users ran the program. The hijacked website urged several users to download a file to update their browsers, which led to reduced computer performance.
Due to the event, flaws such as the usage of default passwords and the lack of protections against brute force assaults were made public. To achieve their objectives, the attacker used malicious JavaScript injection, HTTP requests, and the DNS resolution mechanism. Implementing strong password restrictions, requiring multi-factor authentication, and deploying intrusion detection systems to quickly identify and stop such malicious activity are all advised security measures to reduce future brute force assaults. The website should undergo regular security audits and updates to ensure that it is protected against new threats.

Section 3: Recommend one remediation for brute force attacks
It is essential that yummyrecipesforme.com create an account lockout policy as a corrective action to lessen the danger of future brute force assaults. The effectiveness of brute force assaults can be significantly reduced by configuring the website's authentication system to momentarily lock off user accounts following a specified number of unsuccessful login attempts. This policy would prevent attackers from frequently guessing passwords and gaining unauthorized access by automatically disabling further login attempts from a specific IP address or user account for a certain time. By making it more difficult for brute force attackers to use default or weak passwords, this strategy not only discourages them from attacking the website but also improves its overall security posture. Regularly monitoring and adjusting the account lockout parameters based on emerging threats and attack patterns will further strengthen the website's defenses against brute force attacks.