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

Based on the provided DNS & HTTP traffic log, the network protocol involved in the incident is the Hypertext Transfer Protocol (HTTP), port 80. The log captures HTTP requests and responses between the source computer and the web server, indicating the transfer of web page content and the download of the malicious executable file.

Section 2: Document the incident

- **Source of Attack:** Disgruntled baker
- **Attack Method:** Brute force attack to guess the default password of the admin account
- **Impact:** Modification of website source code, embedding of malicious JavaScript function, unauthorized access to the admin panel, redirection of visitors to a fake website, availability of paid recipes for free
- **Discovery:** Customer complaints and inability of website owner to access the admin panel
- **Evidence:** Customer testimony, website owner testimony, tcpdump log, senior cyber security professional analysis of website source code and downloaded file

A security incident occurred at the Yummyrecipesforme.com website where a disgruntled baker executed a brute force attack to gain unauthorized access to the website's admin panel. The attacker successfully guessed the default password for the administrative account and proceeded to modify the website's source code. This modification included embedding a JavaScript function that prompted visitors to download and run an executable file. Upon running the file, customers were redirected to a fake version of the website (greatrecipesforme.com) where the seller's recipes were available for free. Multiple customers reported slow-running computers and a change in the website's address.

Using a sandbox environment, an investigation was conducted to safely test the website. During the investigation, network traffic was captured using tcpdump. Upon accessing the website, it prompted to download a file that claimed to update the browser. After accepting and running the file, the browser redirected to another website. Instead of being routed to the original site, www.yummyrecipesforme.com, it routed to www.greatrecipesforme.com.

Further examination by a senior cybersecurity professional involved reviewing the source code of both websites and the downloaded file. It was determined that the attacker had injected malicious code into the Yummyrecipesforme.com website, triggering the download prompt disguised as a browser update. Additionally, the website owner's account had been compromised, likely through a brute force attack, resulting in unauthorized changes to the admin password. The execution of the downloaded file led to the compromised state of the customers' computers, causing slow performance issues.

Section 3: Recommend one remediation for brute force attacks

Understanding that the disgruntled baker was able to guess the password because the admin password was still set to the default password, we can definitively recommend enforcing a strong password policy for administrators. This alone would not prevent a brute force attack. One remediation to prevent future brute force attacks, is to implement two-factor authentication (2FA) for all user accounts, including the admin account. 2FA adds an additional layer of security by requiring users to provide a second authentication factor, such as a unique code sent to their mobile device, in addition to the password. This measure significantly reduces the likelihood of successful brute force attacks as even if the attacker guesses the password, they will still need the second factor to gain access.