Security incident report

5th February 2025

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.

Jefferson Yankson

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 noticed 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.

Jefferson Yankson

Security incident report

Section 1: Identify the network protocol involved in the incident
The traffic log shows that the protocol involved in the current incident is the Hypertext Transfer Protocol (HTTP) since the issue was with accessing the web server for “www.yummyrecipesforme.com” and the web server deals with HTTP traffic. When we ran the tcpdump and accessed “www.yummyrecipesforme.com,” the tcpdump log file showed the usage of HTTP when contacting the web server.

Section 2: Document the incident
At 2:18 p.m., a disgruntled employee compromised the website of the company www.yummyrecipesforme.com. The malicious activity led customers to reach out to the helpdesk of YummyRecipes with complaints that the website had prompted them to download an extra file to access free recipes. After downloading the file, customers who ran it claimed the address of their website had changed, and their devices started to run slower. The website owner tried to log in to access the admin panel but was unable to. They then contacted the hosting service company and reported the incident. After the incident was presented to the cybersecurity team, we performed operations in a sandbox environment to observe the incident and also prevent any interference in our internal network. I ran the network packet analyzer and entered the URL. Shortly after, I was prompted to download a file. I accepted the file, downloaded it, and ran it. The file redirected me to a different URL, “www.greatrecipesforme.com,” which contains malware. The log file showed that: 1. The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server.

Jefferson Yankson

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.

Several investigations confirmed the website had been compromised. A senior analyst examined the source code of the website and realized it had been tampered with. The disgruntled employee embedded a JavaScript function into the source code to prompt users to download the malicious file any time they visited the website. The team believes the situation occurred due to a brute force attack since the owner of the website stated they had been locked out of their administrative account.

Section 3: Recommend one remediation for brute force attacks

YummyRecipes should implement new password policies and access controls in their organization. This means standardizing good practices when setting passwords throughout the business. Policies can include how complex the password should be, setting reminders for password updates, and not reusing old passwords.