Justin Goncalves

7/23/24

Project: Apply OS Hardening Techniques

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

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 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 embedding the malware, the baker 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 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.

Tcpdump logs: os hardening project: tcpdump traffic log
How to read the tcpdump logs: os hardening project: how to read the tcpdump log

Follow the instructions and answer the questions below to complete the activity.

Section 1: Identify the network protocol involved in the incident
The network protocols involved in the incident include DNS (Domain Name System) and HTTP (Hypertext Transfer Protocol), both of which operate over the TCP (Transmission Control Protocol). The incident began with a DNS request from the user's browser to resolve the IP address for yummyrecipesforme.com. The DNS protocol is responsible for translating the human-readable domain name into an IP address that can be used for routing the request across the internet. Once the DNS server returned the IP address, the browser initiated an HTTP request to retrieve the webpage from yummyrecipesforme.com. The HTTP protocol is used for transmitting web pages and data between the user's browser and the web server. The logs show that the web server responded to the HTTP request by prompting the download of a malicious file. Following the execution of this file, the browser issued another DNS request, this time for greatrecipesforme.com, and subsequently made an HTTP request to the new IP address provided by the DNS server. This sequence of events underscores the role of DNS in directing traffic to the correct servers and HTTP in facilitating the actual data transfer between the user and the websites, all of which are underpinned by TCP connections to ensure reliable communication.

Section 2: Document the incident
The incident at yummyrecipesforme.com was a deliberate and malicious attack executed by a former employee who gained unauthorized access to the website's admin panel through a brute force attack. The attacker exploited the use of a default password for the administrative account,

which allowed them to repeatedly guess the correct credentials. Once access was obtained, the attacker modified the website's source code, embedding malicious JavaScript. This script prompted visitors to download an executable file under the pretense of a browser update. Upon downloading and executing the file, users were redirected to a fake website, greatrecipesforme.com, which contained additional malware.

This series of events was confirmed through the analysis of TCPdump logs, which revealed the following sequence: an initial DNS request to resolve the IP address for yummyrecipesforme.com, followed by an HTTP request to load the webpage. The response included the malicious script, which initiated the download of the executable file. Subsequent logs showed a DNS request for greatrecipesforme.com and an HTTP request to this new domain, completing the redirection initiated by the malware. Multiple customers reported the suspicious download prompt and noted that their computers ran slowly after executing the file, indicating the presence of malware. In response, the website owner attempted to log in to the admin panel but was unable to due to the password change implemented by the attacker. The incident was escalated to the hosting provider and cybersecurity analysts for further investigation and mitigation.

Section 3: Recommend one remediation for brute force attacks

To effectively mitigate the risk of brute force attacks, it is highly recommended to implement Multi-Factor Authentication (MFA) for all administrative accounts. MFA adds an additional layer of security by requiring users to provide two or more verification factors to gain access to a resource, such as an account. This can include something the user knows (a password), something the user has (a security token or smartphone), and something the user is (biometric verification, such as fingerprint or facial recognition). Even if an attacker successfully guesses or obtains the password, they would still need the second factor to gain access, which significantly reduces the likelihood of unauthorized access. Implementing MFA not only protects against brute force attacks but also enhances overall security by safeguarding critical accounts and data from various other threats.