Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol used in this incident is HTTP (Hypertext Transfer Protocol). This is the standard protocol for transferring web content. According to the tcpdump log, HTTP traffic was used when accessing both the original website yummyrecipesforme.com and the malicious redirect site greatrecipesforme.com. The attack involved downloading a malicious executable file and redirecting users via HTTP, which operates at the application layer of the TCP/IP model.

Section 2: Document the incident
Several customers contacted the helpdesk at yummyrecipesforme.com to report that the website asked them to download a file to access free recipes. After running the file, their computers became slow and the website URL changed. To investigate, we created a sandbox environment and used tcpdump to capture network traffic while visiting the site. Initially, a connection was made to yummyrecipesforme.com, followed by a prompt to download and run a file. Shortly afterward, a DNS request was made for greatrecipesforme.com, and the browser redirected to that site. A senior analyst reviewed the website source code and found that a JavaScript snippet had been injected. This script prompted the file download and caused the browser redirection. Analysis of the file showed that it contained malware and redirected users to a fake site. The attack was the result of a brute force login attempt, where the attacker guessed the default admin password. Once inside, they modified the site's code to inject malware. There were no protections in place to detect or block repeated login attempts, which allowed the attacker to gain access easily.

Section 3: Recommend one remediation for brute force attacks

I recommend using HTTPS protocol instead of HTTP as it is more secure.

To prevent brute force attacks, I recommend implementing the following two security measures:

1- Multi-Factor Authentication (MFA):
MFA requires users to verify their identity using more than just a password—such as a code sent to their mobile device or email. This means that even if an attacker successfully guesses or steals a password, they will not be able to access the account without the second verification step. MFA significantly reduces the chances of unauthorized access from brute force attacks.

2- Strong Password Policies:
Enforcing strong password requirements helps prevent attackers from easily guessing passwords using common patterns. Recommended policies include:

- Passwords must be at least 8 characters long
- Passwords must include both uppercase and lowercase letters
- Passwords must contain at least one number
- Passwords must include at least one special character.

These rules make passwords harder to guess or crack with brute force tools.

By combining MFA with strong password policies, we can create a robust defense against brute force attacks.