Security incident report

Section 1: Identify the network protocol involved in the incident
Since the reported incident involves the lack of access to the "yummyrecipesforme.com.http" website, the HTTP protocol is involved. The malicious file was downloaded by the browser as an update.

Section 2: Document the incident

Our customers reported that after downloading a file from our website, which was supposed to provide free recipes, their computers significantly slowed down. Following these reports, the server owner attempted to log in and check the issue, but found that they no longer had access.

We decided to investigate this incident. In a secure "sandbox" environment, we launched the website "yummyrecipesforme.com.http" to analyze the logs using the tcpdump program.

It turned out that the file downloaded by customers was malicious software that redirected them to a fake website "greatrecipesforme.com".

Upon reviewing the tcpdump logs, it was evident that the browser initially attempted to connect to the "yummyrecipesforme.com.http" website. Once the connection was established, the file was downloaded and executed. After installation, the traffic was redirected to another website, "greatrecipesforme.com".

A senior specialist, after reviewing the source code of the website and the malicious file, determined that lines of code had been added to the website's code, which were responsible for downloading the malicious file as a browser update. Considering the server owner's lack of access, we suspect that a brute force attack occurred, allowing full access to manipulate the server's code.

Section 3: Recommend one remediation for brute force attacks

To make future attacks of this type more difficult, greater emphasis should be placed on password security within the company. First and foremost, the same passwords as in the past should not be used. It is advisable to change passwords frequently. More often rather than less. Implementing a strong password requirement, which includes the presence of uppercase and lowercase letters, numbers, and special characters, will greatly enhance security. Additionally, we recommend implementing two-factor authentication, which means that in addition to the password, a one-time token will be added, which employees can receive on their smartphone or a dedicated device.