Kicho Yu
2025-02-20

Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident is port 80: Hypertext transfer protocol (HTTP). The issue was to access the yummyrecipesforme.com web server, it is natural to know that requests to web servers for web pages involve HTTP traffic. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident

Several customers contacted the website's helpdesk, reporting that when they visited the website, they were prompted to download and run a file claiming to provide access to new recipes. After running the file, their personal computers began operating slowly. Additionally, the website owner attempted to log into the web server but discovered they were locked out of their administrator account.

To investigate, I used a sandbox environment to safely open the website without impacting the company network. I then ran tcpdump to capture network traffic packets generated by interacting with the website. During this process, I was prompted to download a file claiming to provide free recipes. After downloading and running the file, the browser redirected me to a fake website (greatrecipesforme.com).

Upon inspecting the tcpdump logs, I observed that the browser initially requested the IP address for yummyrecipesforme.com. Once connected via HTTP, I noted that after downloading and executing the file, there was a sudden change in network traffic as the browser requested a new IP address for greatrecipesforme.com. This is related to the log entry with the code HTTP: GET / HTTP/1.1 which shows the browser is requesting data from yummyrecipesforme.com with the HTTP: GET method using HTTP protocol version 1.1. The traffic was subsequently rerouted to this malicious site.

My manager analyzed the source code for both websites and the downloaded file. It was discovered that an attacker had injected code into the legitimate website, prompting users to download a malicious file disguised as a browser update. Given that the website owner reported being locked out of their account, we suspect the attacker used a brute force attack to gain access and change the admin password. The execution of this malicious file ultimately compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks
In order to remediate brute force attacks, everyone in the company including the system admin should have multi-factor authentication (MFA). Since the vulnerability that led to this attack was the attacker's ability to use a default password to log in, it is important that we can rely on another layer of protection — MFA — in addition to a password. This would be a useful authentication when anyone tries to enter the company's web server.