Security incident report

Section 1: Identification of network protocol involved in the incident

The network protocol was involved in the incident was the Hypertext transfer protocol (HTTP).

Section 2: Documenting the incident

Several customers contacted the website’s helpdesk as they experienced slower performance in their personal computers after downloading and running a file from the website.

The cybersecurity analyst used sandbox environment and opened the website without causing any damage to the company’s network. Then, the analyst ran tcpdump to capture the network traffic packets produced by interacting with the website. The website prompted to download a file that shows free recipes. After downloading and running the file, the website address was changed and the analyst was redirected to a similar website named “greatrecipesforme.com”.

The owner of the company explained that the company’s ex-employee took advantage of the company’s administrative password which was the default password by performing brute force attacks. Then, he accessed the source code and embedded a javascript that would prompt the visitors a window on the website to download or run a file, which is actually a malware.

Section 3: Recommended remediation for brute force attacks

Lock the account after a fixed number of failed attempts.

As the attacker tries to figure out the right password, they may take a few attempts to crack it. If the account is locked after a fixed number of failed attempts, it might be very difficult for the attacker to hack the account. The owner of the account will also be notified if there are large number of failed attempts.