Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident is HTTP (Hyper Text Transfer Protocol) which is commonly used for communication between webservers and clients.

In the incident the HTTP protocol was used to get the executable file to be downloaded in the client's computer which then redirected the user to greatrecipeforme.com which was the malicious site.

Section 2: Document the incident

First reported 14:18:32

The issue was first raised when complaints came from customers about when they open the website it made them download a file and after downloading it there computer started to work slowly.

When the admin tried to login they were unable to do it this further clarified that the site was compromised.

The team tries to open the site in a sandbox environment. First the website normally loads, then it prompts the user to download a file after downloading the file malware was installed on the computer .

After reading the Tcpdump logs it showed how the client when requesting for the yummyrecipeforme.com the DNS resolved the request successfully and then the site requested data from the webserver by a GET request after the file that was downloaded executes another request from client goes to ask for the ip of the spoofed site greatrecipeforme.com .

The senior analyst when checked the souce code of the website it showed that a script was injected in the website's source code which made the prompt for user to download free recipes but the file instead redirected the client machine to the fake website, which executed malicious code on the client's device.

Section 3: Recommend one remediation for brute force attacks

The following incident happened due to the admin panel having the default password which allowed the threat actor to brute force the password and then edited the source code to add the file download field.

This attack was successful due to the weak password of the organisation's admin panel, this can be fixed with enforcing strict password policy and also making sure that the password can’t be easily brute forced.

One more measure can be to use 2FA (Two Factor Authentication) which will add another layer of security also the passwords should be frequently updated to prevent unauthorized access to the admin panel.