Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in this incident is Hypertext transfer protocol (HTTP). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. Also, when we ran tcpdump and accessed the yummyrecipesforme.com website the corresponding tcpdump log file showed the usage of the http protocol when contacting the . The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident

Multiple customers had emailed yummyrecipesforme's helpdesk and complained that the company's website had prompted them to download a file to access free recipes. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly.

In response to this incident, the website owner tries to log in to the admin panel but is unable to because they are locked out, therefore they reached out to the website hosting provider.

To address the incident, the cybersecurity analyst uses a sandbox environment to observe the suspicious website behavior. Then they ran the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, it prompted them to download an executable file, which was supposed to be for free recipes. Once downloaded, it was observed that the browser redirects them to a different URL, greatrecipesforme.com, which contains the malware.

The cybersecurity analyst next inspected the logs from the tcpdump. The logs show the that at beginning, the browser initiated a DNS request to the IP address of the yummyrecipesforme.com URL from the DNS server. Once the connection with the website was established over the HTTP protocol, the analyst downloaded the malware and started executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website.

Upon further investigation, the senior cybersecurity professional checks the source code for the website and noticed that javascript code had been added to prompt website visitors to download an executable file, which they thought was supposed to be for free recipes. Since it was confirmed by the website owner that they are unable to access and being locked out from the administrator account, the team believes the hacked used a brute-force attack to take control of the admin account, and changed the admin password.

Section 3: Recommend one remediation for brute force attacks

One remediation for the brute force attacks is to disallow previous passwords from being used. This is due to the reason that the hacker was able to guess the password easily because the admin password was still set to the default password. It’s important that we prevent any old passwords such as default passwords from being used to reset the password. We can also require more frequent password changes.

Additionally, enforcing two-factor authentication (2FA) or MFA will make it more secure from unauthorized access.

Another, is to perhaps limit the number of login attempts, so that any attempts of brute force attacks can easily be avoided.