Cybersecurity Incident Report: Apply OS Hardening Techniques

Identifying the network protocol involved in the incident
The network protocol involved in the incident was Hypertext transfer protocol (HTTP). This is evident from the DNS & HTTP traffic log file resulting from running tcpdump while accessing the yummyrecipesforme.com website to investigate the issue, capture network protocol, and traffic activity. Additionally, our investigation revealed that the suspicious file was transported to end users' systems using the HTTP protocol at the application layer.

Documenting the incident
The team was alerted to a security incident when several customers began to email yummyrecipesforme's helpdesk, stating that when they visited our website, they were prompted to download and run a file to update their browsers. The customers then report that after running the file, the address of the website changed and their personal computers began operating slower. Once these emails were received, the website owner attempted to log into the admin panel, but was unable to due to the credentials then being changed. To investigate the incident, the cybersecurity analyst created a sandbox environment to test the website's suspicious behaviour without impacting the company network. In the sandbox, they launched tcpdump before visiting the website, yummyrecipesforme.com, to capture the network and protocol traffic packets produced when interacting with the website. Once the website loaded, the cybersecurity analyst was prompted to download an executable file to update the browser. They proceeded to accept the download and ran the file. After running the file, the browser then redirected them to a different URL, greatrecipesforme.com, that appeared identical to the website, yummyrecipesforme.com. When inspecting the resulting tcpdump log file, the cybersecurity analyst observed that the browser initially requested the IP address for the website, yummyrecipesforme.com. Then, once the connection with the website was established over the HTTP protocol, the analyst received the download prompt and proceeded to download and execute the file. After executing the file, the logs show a sudden change in network traffic as the browser requested a new IP resolution for the URL, greatrecipesforme.com. The network traffic was then rerouted to the new IP address for the website, greatrecipesforme.com.

The senior cybersecurity professional's analysis of the websites' source code and the suspicious file reveal that a malicious actor had manipulated the website's source code to embed a JavaScript function. This function prompted visitors to download the malicious executable file disguised as a browser update. This file contained a script that then redirected victims' browsers from our website, yummyrecipesforme.com, to, greatrecipesforme.com. Additionally, since the website owner stated that they had lost access to their administrator account, the team suspects the malicious actor used a dictionary attack; a type of brute force attack, to gain access to the account and admin portal and change the admin password and website's source code respectively. Execution of the malicious file compromised the end users' systems.

Recommendation of one remediation for brute force attacks

A new security hardening technique the team plans to implement is two-factor authentication (2FA). This 2FA plan would prevent future brute force attacks from occurring by requiring a second, separate form of authentication. In this plan, authorized users would need to validate their identity by confirming a one-time password (OTP) sent via their email or phone. This, in-turn, would create a barrier of entry for any malicious actor, making it less likely they are able to gain access to the system due to this additional authentication step. Regardless of whether they may guess the correct password.