Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol used in the incident is HTTP (Hypertext transfer protocol). Using tcpdump to check the traffic logs indicate that HTTP was used to install a malicious file into the user's computer which send's the user to a different website than the original one.

Section 2: Document the incident

Several customers reached out to the company, reporting an issue when visiting the website. They described encountering a prompt to install an update, which then redirected them to a different site offering the company's recipes for free. These customers also mentioned a noticeable slowdown in their computer's performance after installing the suspicious file.

Efforts to regain access to the web server were unsuccessful, as the threat actor had altered the password following unauthorized access to the system. To investigate the suspicious file, a cybersecurity analyst used a virtual sandbox. The analyst visited the website, establishing an HTTP protocol connection and proceeded to install the file, which was presented as a routine browser update. Examination of the logs show a shift in network traffic, redirecting the analyst to the fake website, "greatrecipesforme.com."

The conclusion drawn by the cybersecurity professional is that the attacker disguised the malicious file as a routine website update. Additionally, the security team believes that a brute force attack likely led to the loss of the administrator's account access, given the current inability to access the web host.

Section 3: Recommend one remediation for brute force attacks

The security team is in the process of implementing Two-Factor Authentication (2FA) to enhance security and prevent potential brute force attacks. 2FA will require that users confirm their identity only after providing two pieces of evidence.