Security incident report

Section 1: Identify the network protocol involved in the incident

The protocol involved in the incident is the Hypertext transfer protocol (HTTP). 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 source computer

Section 2: Document the incident

The cybersecurity incident affecting YummyRecipesForMe began when multiple customers reported suspicious behavior on the company's website. Visitors attempting to access free recipes were prompted to download an executable file, ostensibly to update their browsers. Running the file resulted in their computers slowing down, while their browsers were redirected to a malicious website, GreatRecipesForMe.com. The website owner, unable to access the admin panel, reached out to the hosting provider for assistance. The issue was escalated to cybersecurity analysts, who initiated an investigation.

Sandbox testing revealed that the website had been compromised. Analysis showed that the site's source code contained injected JavaScript designed to prompt visitors to download the malicious file. When executed, the file redirected users to GreatRecipesForMe.com, where additional malware was hosted. Network logs confirmed the sequence of events, including DNS and HTTP requests leading to both YummyRecipesForMe.com and the malicious domain. The senior analyst concluded that the website had been compromised through a brute force attack on the admin account, which had remained set to its default password. The absence of security controls such as rate limiting or account lockouts made the attack successful.

The immediate response involved removing the malicious code, notifying customers of the potential threat, and advising them to secure their systems.

The compromised server was taken offline to prevent further exploitation, and measures were implemented to enhance security. These included using a stronger password, introducing multi-factor authentication, and applying brute force protections to the admin account. Additionally, a forensic analysis of the server was conducted to identify and address other vulnerabilities.

Section 3: Recommend one remediation for brute force attacks

Enforcing two-factor authentication (2FA) will be useful to add an extra layer of protection to user accounts by requiring two forms of verification, such as a password and a unique code sent to your device. It significantly reduces the risk of unauthorized access, even if your password is compromised, this way even when the attacker gains access to old passwords they cannot gain access without having more information