Security incident report

Benjamin Taylor – Google Cybersecurity

Section 1: Identify the network protocol involved in the incident
The protocol that was involved in this incident is HTTP, or Hypertext transfer protocol. Since the issue was with accessing the web server for yummyrecipesforme.com, requests to web servers for web pages include http traffic. When we ran tcpdump while accessing the website, the result logs confirmed that HTTP was the protocol used during the connection. The malicious file was observed being delivered to users' computers through the HTTP protocol at the application layer.

Section 2: Document the incident
Many customers contacted the website's helpdesk, reporting that upon visiting the website they were prompted to download a file providing new recipes when visiting yummyrecipesforme.com. After downloading, their computers began running much slower than usual. The owner of the website was locked out of the admin account, suggesting a brute-force attack was taking place. Through tcpdump, it was observed the site used HTTP and redirected to greatrecipesforme.com after the file had been executed. Analysis afterwards revealed that malicious code had been injected into the side, prompting users to download a fake browser update. This file took control over the users' devices and rerouted all traffic to the malicious site.

Section 3: Recommend one remediation for brute force attacks
To protect against future brute force attacks, the team plans to disallow reuse of previous passwords in order to prevent attackers from exploiting them during password resets. There will also be more frequent password updates to limit the window of opportunity for unwanted access. Also, implementing 2FA (two-factor authentication) will add a strong security layer by requiring users to verify their identity through not only a password but also a one-time code sent to their phone or email, hopefully keeping attackers out.