Security incident report

Section 1: Identify the network protocol involved in the incident

The incident involved the disruption of the Hypertext Transfer Protocol (HTTP). By utilizing tcpdump and visiting the yummyrecipesforme.com website to identify the issue, record the protocol, and log traffic activity in both DNS and HTTP, we gathered the necessary evidence to arrive at this determination. It was observed that the malicious file was transferred to users' computers via the HTTP protocol at the application layer.

Section 2: Document the incident

Multiple customers reached out to the website owner, reporting that when they visited the site, they were presented with a request to download and execute a file, purportedly for updating their web browsers. Subsequently, their personal computers experienced a significant decrease in performance. Additionally, the website owner encountered difficulties logging into the web server as their account had been locked.

To investigate the situation, a cybersecurity analyst employed a sandbox environment to assess the website's functionality without impacting the company's network. The analyst then utilized tcpdump to record network and protocol traffic packets generated through interactions with the website. While exploring the website, the analyst encountered a prompt to download a file promising a browser update, which they accepted and executed. This action led the browser to redirect the analyst to a fraudulent website, greatrecipesforme.com, which bore an uncanny resemblance to the original site, yummyrecipesforme.com.

Upon reviewing the tcpdump log, the cybersecurity analyst noted that the browser initially requested the IP address for the yummyrecipesforme.com site. After establishing a connection with the website via the HTTP protocol, the analyst recalled downloading and running the file. The log entries exhibited a sudden shift in network traffic as the browser sought a new IP resolution for the greatrecipesforme.com URL, subsequently rerouting the traffic to the new IP address associated with the greatrecipesforme.com website.

Subsequently, a senior cybersecurity professional scrutinized the source code of both websites and the downloaded file. This examination revealed that an attacker had manipulated the website by inserting code that prompted users to download a malicious file disguised as a browser update. Given the website owner's claim of being locked out of their administrative account, it is suspected that the attacker gained unauthorized access via a brute force attack, subsequently altering the admin password. The execution of the malicious file compromised the end-users' computers.

Section 3: Recommend one remediation for brute force attacks

To bolster security and thwart potential brute force attacks, the team intends to introduce a two-factor authentication (2FA) mechanism. This 2FA strategy will entail an extra layer of verification for users, obliging them to confirm their identity by entering a one-time password (OTP) sent either to their email address or mobile phone. Once users successfully authenticate themselves by providing their login credentials in conjunction with the OTP, they will be granted access to the system. This approach significantly mitigates the risk of malicious actors gaining unauthorized entry via brute force attacks, as it necessitates an additional level of authorization beyond just a username and password.