Security incident report

Section 1: Identify the network protocol involved in the incident

The incident involved the Hypertext Transfer Protocol (HTTP). Since accessing the web server for yummyrecipesforme.com requires HTTP, tcpdump logs showed the HTTP protocol being used when contacting the website. The malicious link is transmitted to users' computers using HTTP at the application layer.

Section 2: Document the incident

Several customers reported to the website's helpdesk that upon visiting the site, they were prompted to download and execute a file purportedly containing access to new recipes. Since then, their personal computers have been experiencing significant performance degradation. The website owner attempted to log into the web server but was subsequently locked out of their account.

To investigate the incident, a cybersecurity analyst employed a sandbox environment to access the website without compromising the company's network infrastructure. Subsequently, tcpdump was utilized to capture network traffic during interactions with the website.

The analyst was prompted to download a file claiming it would provide access to complimentary recipes. Upon accepting the download, the file executed, redirecting the user to a phishing website (greatrecipesforme.com).

Inspecting the tcpdump log, the analyst observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Upon establishing an HTTP connection, the analyst recalled executing the malicious file. The logs revealed a sudden alteration in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL. Subsequently, the network traffic was redirected to the new IP address associated with the greatrecipesforme.com website.

The senior cybersecurity professional analyzed the source code for both the websites and the downloaded file. They discovered that an attacker had manipulated the website to incorporate code that prompted users to download a malicious file disguised as a browser update. Given the website owner's mention of being locked out of their administrator account, the team surmises that the attacker employed brute-force techniques to gain unauthorized access to the account and subsequently alter the administrator password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommend one remediation for brute force attacks

To mitigate the risk of brute-force attacks, the team has devised a comprehensive security strategy. A pivotal measure involves prohibiting the reuse of previously compromised passwords. The vulnerability exploited during the attack was the attacker’s ability to gain access using a default password. Consequently, it is imperative to prevent the utilization of any outdated passwords, including default passwords, for password reset procedures.

In addition, the team has implemented a policy of more frequent password updates. This proactive approach significantly reduces the likelihood of unauthorized access to passwords, as any compromised credentials will be rendered ineffective upon prompt updates.

Furthermore, the implementation of two-factor authentication (2FA) serves as a robust security measure. 2FA necessitates authentication through both a password and a one-time passcode (OTP) sent via email or phone. Upon successful verification of identity through login credentials and OTP, users gain access to the system. This additional layer of authentication effectively hinders malicious actors attempting to exploit brute-force attacks, as they require additional authentication to gain unauthorized access.