Apply OS hardening techniques

Section 1: Identify the network protocol involved in the incident

Hypertext transfer protocol (HTTP) is the protocol that was impacted by the incident. The information required to draw this conclusion came from running tcpdump, visiting the yummyrecipesforme.com website, and identifying the issue. These actions allowed us to record protocol and traffic activity in a DNS & HTTP traffic log file. At the application layer, the malicious file is seen being transferred to the users' computers over the HTTP protocol.

Section 2: Document the incident

Numerous users complained to the website's owner that they were forced to download and run a file when they visited the site because their browsers needed to be updated. Since then, the performance of their personal computers has been poor. The owner of the website attempted to get into the web server but discovered they had been locked out of their account.

The website was tested in a sandbox environment by the cybersecurity expert without affecting the corporate network. To record the network and protocol traffic packets generated by interacting with the website, the analyst then used tcpdump. The analyst agreed to the request to download a file that would allegedly update the user's browser and then execute it. The analyst was then sent by the browser to a false website (greatrecipesforme.com) that had the exact same design as the real website (yummyrecipesforme.com).

When the cybersecurity expert looked at the tcpdump record, he or she saw that the browser had first queried the yummyrecipesforme.com website's IP address. The analyst remembered downloading and running the file after connecting to the website using the HTTP protocol. The logs revealed a dramatic shift in network activity when the browser asked for a new IP address to resolve the greatrecipesforme.com URL. A new IP address for the website greatrecipesforme.com was then chosen to receive network traffic.

The senior cybersecurity expert examined the downloaded file and the website's source code. The analyst found that a hacker had added code to the website by manipulating it, prompting users to download a malicious file that was passed off as a browser update. The team thinks the attacker performed a brute force assault to access the account and modify the admin password because the website owner claimed they had been locked out of their administrator account. The PCs of the end users were infected when the malicious file was executed.

Section 3: Recommend one remediation for brute force attacks

Two-factor authentication (2FA) is one security solution the team intends to use to defend against brute force attacks. Users will also be required to confirm a one-time password (OTP) issued to either their email address or phone number as part of this 2FA strategy in order to verify their identity. The user will have access to the system once they have verified their identity using their login information and the OTP. A brute force attack by a bad actor is unlikely to succeed since the system needs extra authorization.