APLICACIÓN DE TÉCNICAS DE REFORZAMIENTO DEL SISTEMA OPERATIVO

Sección 1: Identificación del Protocolo de Red Involucrado
El protocolo implicado en el incidente fue el protocolo de transferencia de hipertexto (HTTP). Para detectar el problema, se utilizó la herramienta tcpdump y se accedió al sitio web yummyrecipesforme.com, registrando la actividad del tráfico de DNS y HTTP. Esto permitió confirmar que un archivo malicioso estaba siendo transmitido a los dispositivos de los usuarios a través del protocolo HTTP en la capa de aplicación.

Sección 2: Documentación del Incidente
Varios clientes notificaron al propietario del sitio web que, al visitar la página, se les solicitaba descargar y ejecutar un archivo con la supuesta intención de actualizar sus navegadores, lo que resultó en un rendimiento más lento de sus computadoras. El propietario intentó acceder al servidor, pero encontró sus cuentas bloqueadas. Un analista de ciberseguridad empleó un entorno controlado (sandbox) para probar el sitio web sin comprometer la red corporativa. Al ejecutar tcpdump, se capturaron los paquetes de tráfico de red y protocolos durante la interacción con el sitio. El analista fue invitado a descargar un archivo que pretendía ser una actualización del navegador, que fue aceptado y ejecutado. El navegador posteriormente redirigió al analista a un sitio web falso (greatrecipesforme.com) que imitaba el sitio original (yummyrecipesforme.com). Al revisar los registros de tcpdump, el analista observó que el navegador inicialmente solicitó la dirección IP de yummyrecipesforme.com. Tras establecer la conexión mediante HTTP, el tráfico mostró un cambio abrupto cuando el navegador buscó una nueva resolución IP para la URL greatrecipesforme.com, redirigiendo el tráfico a la nueva IP de este sitio. Un profesional sénior de ciberseguridad examinó el código fuente de ambos sitios y el archivo descargado, descubriendo que un atacante había modificado el sitio web para incluir código que incitaba a los usuarios a descargar un archivo malicioso disfrazado de actualización del navegador. Dado que el propietario del sitio reportó haber sido bloqueado de su cuenta de administrador, el equipo sospecha que el atacante empleó un ataque de fuerza bruta para acceder y cambiar la contraseña de la cuenta.

Sección 3: Recomendaciones para Prevenir Ataques de Fuerza Bruta

Como medida preventiva contra futuros ataques de fuerza bruta, se recomienda implementar autenticación de dos factores (2FA). Este sistema requerirá que los usuarios verifiquen su identidad mediante una contraseña única (OTP) enviada a su correo electrónico o teléfono. Así, incluso si un atacante intenta un ataque de fuerza bruta, no podrá acceder al sistema sin la autenticación adicional proporcionada por la OTP.