INFORME DEL INCIDENTE DE SEGURIDAD

Sección 1: Identificación del Protocolo de Red Involucrado
En el incidente, se identificó que el protocolo afectado fue el protocolo de transferencia de hipertexto (HTTP). La utilización de la herramienta tcpdump y el acceso al sitio web yummyrecipesforme.com permitieron detectar el problema y registrar la actividad de tráfico en un archivo que contenía datos de DNS y HTTP. Esto proporcionó la evidencia necesaria para determinar que un archivo malicioso estaba siendo distribuido a los usuarios a través del protocolo HTTP en la capa de aplicación.

Sección 2: Documentación del Incidente
Varios clientes informaron al propietario del sitio web que, al visitar el sitio, se les solicitaba descargar y ejecutar un archivo para supuestamente actualizar sus navegadores, lo que resultó en un rendimiento lento de sus computadoras. El propietario del sitio web intentó acceder al servidor, pero descubrió que sus cuentas habían sido bloqueadas. Un analista de ciberseguridad realizó pruebas en un entorno controlado (sandbox) para evitar afectar la red corporativa. Al ejecutar tcpdump, capturó los paquetes de tráfico y protocolos asociados al sitio web. Durante la prueba, se le pidió al analista descargar un archivo que pretendía ser una actualización del navegador, el cual fue aceptado y ejecutado. Posteriormente, el navegador redirigió al analista a un sitio web falso (greatrecipesforme.com) que imitaba al original (yummyrecipesforme.com). El análisis del registro de tcpdump reveló que el navegador inicialmente solicitó la dirección IP de yummyrecipesforme.com y, tras establecer la conexión vía HTTP, ocurrió un cambio repentino en el tráfico, redirigiendo a una nueva IP asociada con greatrecipesforme.com. Un profesional sénior de ciberseguridad analizó el código fuente de los sitios y el archivo descargado, descubriendo que un atacante había alterado el sitio web para incluir código que inducía a los usuarios a descargar un archivo malicioso disfrazado de actualización del navegador. Dado que el propietario del sitio informó que su cuenta de administrador fue bloqueada, se sospecha que el atacante utilizó 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 de seguridad contra futuros ataques de fuerza bruta, se planea implementar la 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. De esta manera, incluso si un atacante intenta un ataque de fuerza bruta, no podrá acceder al

Sección 3: Recomendaciones para Prevenir Ataques de Fuerza Bruta
sistema sin la autenticación adicional proporcionada por la OTP.