

# Informe del incidente de seguridad

## Sección 1: Identifica del protocolo de red involucrado en el incidente

El protocolo afectado en el incidente es el protocolo de transferencia de hipertexto (HTTP). La ejecución de tcpdump y el acceso al sitio web yummyrecipesforme.com para detectar el problema y capturar el protocolo y la actividad de tráfico en un archivo de registro de tráfico DNS y HTTP proporcionó la evidencia necesaria para llegar a esta conclusión. Se observa que el archivo malicioso se transporta a las computadoras de los/las usuarios/as utilizando el protocolo HTTP en la capa de aplicación.

## Sección 2: Documenta el incidente

Varios/as clientes se pusieron en contacto con el/la propietario/a del sitio web indicando que, al visitar dicho sitio, se les pidió descargar y ejecutar un archivo que les pedía que actualizaran sus navegadores. Sus computadoras personales funcionan con lentitud desde entonces. El/la propietario/a del sitio web intentó iniciar sesión en el servidor web, pero advirtió que sus cuentas estaban bloqueadas.

La/el analista de ciberseguridad utilizó un entorno controlado (sandbox) para probar el sitio web sin afectar la red de la empresa. Luego, ejecutó tcpdump para capturar los paquetes de tráfico de red y protocolo producidos al interactuar con el sitio web. Se le pidió al/ a la analista que descargara un archivo que supuestamente actualizaría el navegador del usuario, este/a aceptó la descarga y lo ejecutó. El navegador luego redirigió al/a la analista a un sitio web falso (greatrecipesforme.com) que se veía idéntico al sitio original (yummyrecipesforme.com).

El/la analista de ciberseguridad inspeccionó el registro de tcpdump y observó que, inicialmente, el navegador solicitó la dirección IP para el sitio web yummyrecipesforme.com. Una vez que se estableció la conexión con el sitio web a través del protocolo HTTP, el/la analista recordó descargar y ejecutar el archivo. Los registros mostraron un cambio repentino en el tráfico de red cuando el navegador solicitó una nueva resolución IP para la URL greatrecipesforme.com. El tráfico de red fue redirigido a la nueva dirección IP para el sitio web greatrecipesforme.com.

El/la profesional sénior de ciberseguridad analizó el código fuente de los sitios web y el archivo descargado. El/la analista descubrió que un/a atacante había manipulado

el sitio web para agregar código que llevó a los/las usuarios/as a descargar un archivo malicioso disfrazado de actualización del navegador. Como el/la propietario/a del sitio web declaró que le habían bloqueado su cuenta de administrador, el equipo cree que la/el responsable utilizó un ataque de fuerza bruta para acceder a la cuenta y cambiar la contraseña del administrador. La ejecución del archivo malicioso comprometió las computadoras de los/las usuarios/as finales.

### **Sección 3: Recomienda una solución para los ataques de fuerza bruta**

Una medida de seguridad que el equipo planea implementar para protegerse contra los ataques de fuerza bruta es la autenticación de dos factores (2FA). Este plan 2FA incluirá un requisito adicional para que los/las usuarios/as validen su identificación confirmando una contraseña única (OTP) enviada a su correo electrónico o teléfono. Una vez que el/la usuario/a confirme su identidad a través de sus credenciales de inicio de sesión y la OTP, obtendrá acceso al sistema. Cualquier agente de amenaza que intente un ataque de fuerza bruta probablemente no obtendrá acceso al sistema porque requiere autorización adicional.