**Informe de incidente de seguridad**

**Sección 1: Identificar el protocolo de red involucrado en el incidente**

El protocolo implicado en el incidente es el protocolo de transferencia de hipertexto (HTTP), dado que el problema fue con el acceso al servidor web de yummyrecipesforme.com. Además, cuando ejecutamos tcpdump y accedemos al sitio web, el archivo de registro de tcpdump correspondiente mostró el uso del protocolo http al contactar con el archivo. Se observa que el archivo malicioso se transporta a las computadoras de los usuarios utilizando el protocolo HTTP en la capa de aplicación.

**Sección 2: Documentar el incidente**

Varios clientes se pusieron en contacto con el servicio de asistencia técnica del sitio web y dijeron que cuando accedían al sitio web, se les pedia descargar y ejecutar un archivo que contenía acceso a nuevas recetas. Desde entonces, sus computadoras personales han estado funcionando lentamente. El propietario del sitio web intentó iniciar sesión en el servidor web pero notó que su cuenta estaba bloqueada.

Se utilizó un entorno sandbox para abrir el sitio web sin afectar la red de la empresa, luego ejecutó tcpdump para capturar los paquetes de tráfico de red producidos al interactuar con el sitio web, se descargó el archivo que afirmaba darle acceso a recetas gratuitas. Tras ello, el navegador lo redirigió a un sitio web falso (greatrecipesforme.com).

Se inspeccionó el registro tcpdump observando que el navegador inicialmente solicitaba la dirección IP del sitio web yummyrecipesforme.com, sin embargo una vez descargado y ejecutado el archivo, los registros mostraron un cambio repentino en el tráfico de la red, solicitando una nueva dirección IP para la URL greatrecipesforme.com. Luego, el tráfico de la red se redirigió a la nueva dirección IP del sitio web greatrecipesforme.com.

El profesional sénior de ciberseguridad analizó el código fuente de los sitios web y el archivo descargado. El analista descubierto que un atacante había manipulado el sitio web para agregar código que incitaba a los usuarios a descargar un archivo malicioso disfrazado de actualización del navegador. Dado que el propietario del sitio web declaró que se le había bloqueado el acceso a su cuenta de administrador, el equipo cree que el atacante utilizó un ataque de fuerza bruta para acceder a la cuenta y cambiar la contraseña de administrador.

**Sección 3: Recomendar una solución para ataques de fuerza bruta**

Una medida de seguridad que el equipo planea implementar para protegerse contra ataques de fuerza bruta es no permitir el uso de contraseñas anteriores, dado que la vulnerabilidad que provocó este ataque fue la capacidad del atacante de utilizar una contraseña predeterminada para iniciar sesión, es importante que evitemos que se utilicen contraseñas antiguas, como las predeterminadas, para restablecer la contraseña. Otra medida de apoyo es exigir contraseñas más largas. Las contraseñas de 15 caracteres o más ofrecen una mayor protección contra ataques de fuerza bruta. Otra solución útil es implementar la autenticación de dos factores (2FA), puesto que requiere autenticación mediante una contraseña y confirmando un código de acceso de un solo uso (OTP) enviado a su correo electrónico o teléfono.