# Informe del incidente de seguridad

|  |
| --- |
| Sección 1: Identificación del protocolo de red involucrado en el incidente |
| El protocolo utilizado es protocolo de Aplicación y de transporte, ya que se ha realizado una petición http, resolución de DNS cuando se solicitó a la pagina |
|

|  |
| --- |
| Sección 2: Documentación del incidente |
| El panadero X ha decidido realizar publicaciones de las recetas más vendidas de nuestra página, donde el ha realizado un ataque de fuerza bruta con el usuario administrador, logrando con ello acceder al panel de administración, realizando una modificación en el códig fuente del sitio, ha incrustado una función de descarga y redirecciÃ³n en el lenguaje JavaScript, donde cada usuario que hace una petición http a nuestro sitio, inmediatamente le pide actualizar el navegador, descargando un malware y haciendo una redirección al host **192.0.2.172 correspondiente a greatrecipesforme.com sitio donde se encuentran publicadas las recetas de manera gratuita.** |

|  |
| --- |
| Sección 3: Recomendación de una solución para los ataques de fuerza bruta |
| Para evitar incurrir en estos ataques de fuerza bruta será:  Crear otro usuario con todos los permisos administrativos. Dar de baja al usuario con permiso administrador. Colocar un límite a nivel de programación para intentos de acceso al panel administrativo. |