# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Para comenzar, el protocolo de red usado en este incidente es el protocolo HTTP asociado al puerto 80 de red. Este podría ser el apartado web que realiza la descarga del archivo malicioso con el que tendremos la redirección al sitio web que ha sido controlado por los ciberdelincuentes.  En el log podemos observar de qué manera se realiza la bajada del archivo malicioso : **HTTP: GET / HTTP/1.1** | |
|

| **Section 2: Document the incident** |
| --- |
| Inicialmente, los usuarios intentaron acceder a los habituales servicios de recetas y libros de cocina del sitio web. Sin embargo, esta vez, se encontraron con una solicitud inusual: para continuar navegando, debían descargar y ejecutar un archivo malicioso que, al hacerlo, se instalaría en sus dispositivos.  Este script malicioso redirecciona el tráfico de clientela a otro dominio en manos del ciberdelincuente y así poder hacerse con los datos de las víctimas.  El nombre del dominio pasó de llamarse “[yummyrecipesforme.com](http://yummyrecipesforme.com)” a “[greatrecipesforme.com](http://greatrecipesforme.com)”.  Muchos de los usuarios debido al software malicioso comenzaron a tener problemas con sus dispositivos, notando que estos eran bastante lentos y no hacían una función óptima, por lo que, muchos de ellos tuvieron la necesidad de abrir incidencias al departamento técnico IT de la página web.  Tras una investigación por parte del equipo a fondo, pudieron comprobar que los sistemas habían sido atacados mediante el método de fuerza bruta pudiendo acceder al host web, cambiando credenciales y elevando sus privilegios, además, cambió el código fuente para que los usuarios que querían acceder a la página web obtuvieran una descarga directa al software malicioso.  Al abrir este software eran redireccionados a la misma página pero esta vez modificada por el ciberdelincuente apuntando a un dominio y host web totalmente diferentes.  Los técnicos analistas del departamento, crearon un laboratorio de pruebas para comprobar y analizar el software malicioso creado por el atacante. A este entorno se le llama “Sandbox” y permitió la ejecución y análisis del virus inyectado. En resolución, la persona atacante del sitio web puede elevar y ejecutar sus permisos de usuario dentro del host web e instalar software malicioso de manera remota dentro de los equipos de los clientes. Obteniendo así información confidencial y provocando un gran impacto en la confidencialidad y fidelidad de los clientes con el servicio web. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Para evitar ataques de fuerza bruta un sistema debe cumplir con los siguientes requerimientos que se mencionan a continuación:   * Limitar el número de intentos de inicio de sesión por IP de dispositivo. * Uso de captcha para comprobación de inicio de sesión humano. * Habilitación de métodos de seguridad como MFA o 2FA. * Contraseñas de mínimo 12 caracteres o más. * Asegurarnos de que los usuarios usan HTTPS en lugar de HTTP. * SSH con Claves Públicas: Para el acceso remoto a servidores, utilizar la autenticación basada en claves públicas en lugar de contraseñas. |