# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| El protocolo que se ve involucrado en el incidente es: el Protocolo de Aplicación.  Puerto involucrado es el 80, al ver saturación de datos. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| El incidente ocurre a las 14:18:32hrs desde la IP your.machine.52444  El incidente fue notificado por varios clientes a traves de correos electronicos, quienes notificaron que al acceder a las recetas gratuitas les obligaba a desacargar un archivo y posterior a ello sus equipos de uso personal empezaron a funcionar lentamente.  Como respuesta a este incidente el equipo de seguridad ejecutó el analizador de protocolos de red tcpdump así identificar que protocolos se han visto comprometidos y determinar cual ha sido la superficie del daño que ha abarcado este ataque.  Al analizar la situación se ha detectado que se ha debido a un ataque de fuerza bruta, en el cual se a forzado la identificación de contraseñas para acceder sin autorización al alojamiento del sitio web de la empresa y así redirigir a los visitantes de la página web a una distinta a la de yummyrecipesforme.com y posterior instalar un script (codigo malisioso) para probocar un funcionamiento lento en sus ordenadores personales.  Este incidente se ha debido al acceso del alojamiento web de un actor malintencionado desde nuestras instalaciones, que ha perjudicado el funcionamiento de la pagina web afectando a su vez a nuestros clientes. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Se recomienda establecer en la empresa la siguiente medida de Endurecimiento de Seguridad Autenticación en dos factores (2FA) ante ataques de fuerza bruta futuros.  Esta medida ayudará a identificar inicio de sesiones y obligará a verificar si la sesión es autentica, lo que ayudará a autorizar o no el uso del equipo de la empresa y se evite la suplantación de identidad. |