# Informe del incidente de seguridad

|  |
| --- |
| Sección 1: Identificación del protocolo de red involucrado en el incidente |
| El incidente de seguridad involucra el uso de varios protocolos de red en la capa de aplicación y de transporte. En primer lugar, se identificó el protocolo **DNS** como responsable de la resolución inicial de nombres de dominio, al traducir la URL yummyrecipesforme.com a la dirección IP correspondiente. Posteriormente, se observó el establecimiento de una conexión **TCP**, necesaria para la transmisión de datos entre cliente y servidor. Finalmente, el contenido fue entregado a través del protocolo **HTTP**, mediante solicitudes **GET** sobre el puerto 80.  El análisis realizado con la herramienta **tcpdump** permitió confirmar estos hallazgos, ya que se registraron múltiples paquetes correspondientes a consultas DNS, establecimiento de sesiones TCP y tráfico HTTP. Estos protocolos, especialmente HTTP al no contar con cifrado en este caso, fueron aprovechados por el atacante para manipular la comunicación y distribuir contenido potencialmente malicioso. |
|

|  |
| --- |
| Sección 2: Documentación del incidente |
| El día **14/xx a las 14:18**, se registró la primera interacción con el sitio yummyrecipesforme.com, cuya resolución DNS apuntó a la dirección IP **203.0.113.22**. Seguidamente, el cliente estableció una sesión HTTP/TCP y envió una solicitud **GET /** para acceder al recurso principal del sitio.  No obstante, a las **14:20**, el tráfico de red mostró un comportamiento anómalo: se generó una nueva resolución DNS hacia el dominio **greatrecipesforme.com**, que apuntaba a la IP **192.0.2.172**. De inmediato, el navegador estableció una nueva conexión HTTP/TCP con este servidor. Este cambio abrupto sugiere una **redirección forzada** o manipulación maliciosa en el flujo de resolución de nombres de dominio, lo que permitió que los usuarios fueran enviados a un sitio fraudulento con apariencia similar al legítimo.  Durante el análisis en la captura de **tcpdump**, se observaron fragmentos con **timestamps y flags TCP** que evidencian la secuencia descrita. Además, se identificó que los usuarios eran incitados a descargar un archivo bajo la apariencia de una actualización del navegador, lo que constituye un vector de ataque de tipo **ingeniería social combinada con distribución de malware**.  Como medida inmediata, se recomendó **bloquear temporalmente la dirección IP 192.0.2.172**, así como realizar un análisis más profundo de los **logs del servidor web y de los equipos afectados**, con el fin de determinar el alcance de la infección y validar si existió compromiso de cuentas administrativas. |

|  |
| --- |
| Sección 3: Recomendación de una solución para los ataques de fuerza bruta |
| El análisis sugiere que el atacante pudo haber obtenido acceso privilegiado mediante un **ataque de fuerza bruta** a la cuenta de administrador del sitio web. Para mitigar este tipo de incidentes, se recomienda implementar un conjunto de controles de seguridad:   1. **Limitación de intentos de inicio de sesión** mediante bloqueos temporales, incremento progresivo de tiempos de espera (**backoff exponencial**), uso de **CAPTCHA** y políticas de **rate-limiting** en el nivel de aplicación o a través de un WAF (Web Application Firewall). 2. Incorporar **autenticación multifactor (2FA)**, de modo que además de la contraseña sea necesario validar un **código único (OTP)** enviado al correo electrónico o teléfono del usuario. 3. Establecer un sistema de **monitoreo y alertas** que detecte intentos reiterados de acceso fallido, con el fin de responder de manera temprana a patrones que indiquen ataques automatizados.   Con estas medidas, se refuerza la protección contra accesos no autorizados y se reduce la probabilidad de éxito de futuros intentos de fuerza bruta.  . |