Informe del incidente de seguridad

Sección 1: Identificación del protocolo de red involucrado en el incidente
El protocolo que se vio afectado es el de HTTP, al momento de cargar el contenido de la pagina se inicia una descarga de malware no autorizada, al mismo tiempo te redirige a una url parecia a la original, pasa de esta url (yummyrecipesforme.com) -> (greatrecipesforme.com.).

Sección 2: Documentación del incidente
Un Hacker no etico realizo ataques de fuerza bruta porbando multiples contraseñas predeterminadas logrando ingresar al panel administrativo e inserto un codigo malicioso que descarga un malware y te redirige a una url parecida. Varios clientes reportaron el extraño comportamiento y lo reportaron, inmediatamente varios analista de ciberseguridad al ingresar a la url junto a un registro tcpdump revelaron que al ingresar: - Solicitud de Resolucion DNS (Exitosa) - Conexion con protocolo TCP (Exitosa) - Traferencia o carga de datos con el protocolo HTTP (Exitosa) Este ultimo es el que se ve afectado ya que al finalizar la carga del contenido se inicia una desarga maliciosa y un redireccionamiento de pagina, este comportamiento es la que resulta manipulada por parte del atacante, una vez redireccionado a otra url con un contenido similar en todo aspecto se observa los mismo pasos, Resolucion DNS -> Conexion TCP y carga la informacion de la pagina con el protocolo HTTP.

Sección 3: Recomendación de una solución para los ataques de fuerza bruta
Para poder evitar que este tipo de ataques lo mas recomendable hacer es implementar: Políticas de contraseña que aumenta la complejidad al momento de escribir

una contraseña.
Autenticación de múltiples factores (MFA) y autenticación de dos factores (2FA) se realiza al utilizar una combinación de factores de autenticación, nombre de usuario y contraseña, huellas dactilares, reconocimiento facial, etc.
CAPTCHA y reCAPTCHA, Prueba de Turing Pública y Automatizada para Diferenciar entre Máquinas y Humanos, reCAPTCHA: Es una versión mejorada de CAPTCHA, ayudan a prevenir el acceso automatizado mediante scripts y programas.