Una táctica recién descubierta conocida como «SMTP smuggling» (contrabando SMTP) puede ser aprovechada por delincuentes cibernéticos para enviar mensajes de correo electrónico con remitentes falsificados, evadiendo las protecciones de seguridad.

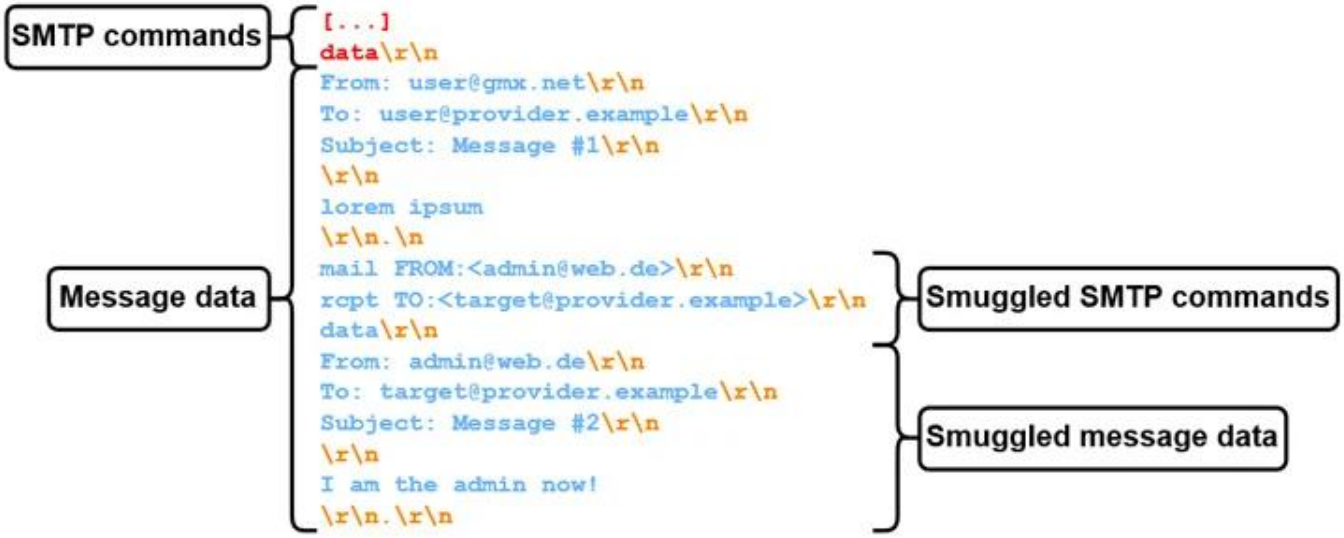
> Según Timo Longin, un experto en seguridad de SEC Consult, *«Los ciberdelincuentes podrían explotar servidores SMTP desprotegidos en diversas ubicaciones para emitir mensajes de phishing desde direcciones de correo fraudulentas».*

SMTP, un estándar en la comunicación en línea, facilita el envío y la recepción de correos electrónicos a través de sistemas conectados. Cuando un usuario intenta enviar un correo electrónico, se establece una comunicación directa con el servidor SMTP para entregar el mensaje al destinatario.

Después, el servidor utiliza un agente especializado (MTA) para validar el destino del correo. Si el dominio del receptor difiere del emisor, el sistema consulta una base de datos (DNS) para localizar el servidor de correo adecuado y completar el proceso de entrega.

El truco del contrabando SMTP se basa en inconsistencias presentes cuando distintos servidores SMTP procesan información de forma desigual, lo que podría permitir a delincuentes manipular los datos del mensaje, insertar comandos no autorizados o incluso generar mensajes adicionales.

Este método recuerda a otra táctica conocida como *«HTTP request smuggling»,* que se aprovecha de las variaciones en el procesamiento de encabezados HTTP para introducir solicitudes engañosas en flujos de datos.



Se han identificado vulnerabilidades en sistemas de mensajería de Microsoft, GMX y Cisco, permitiendo a los atacantes emitir mensajes desde dominios ficticios. Implementaciones SMTP de Postfix y Sendmail también se ven comprometidas.

Estas debilidades posibilitan el envío de mensajes fraudulentos que, a primera vista, parecen legítimos, eludiendo mecanismos de autenticación como DKIM, DMARC y SPF.

Aunque Microsoft y GMX han tomado medidas correctivas, Cisco ha considerado las fallas como «*funcionalidades*» y no tiene planes de alterar su configuración preestablecida, lo que mantiene vulnerables ciertos sistemas a ataques SMTP.

Como recomendación, SEC Consult sugiere a los usuarios de Cisco modificar sus ajustes para minimizar el riesgo de recibir correos electrónicos fraudulentos que superen las comprobaciones de seguridad.