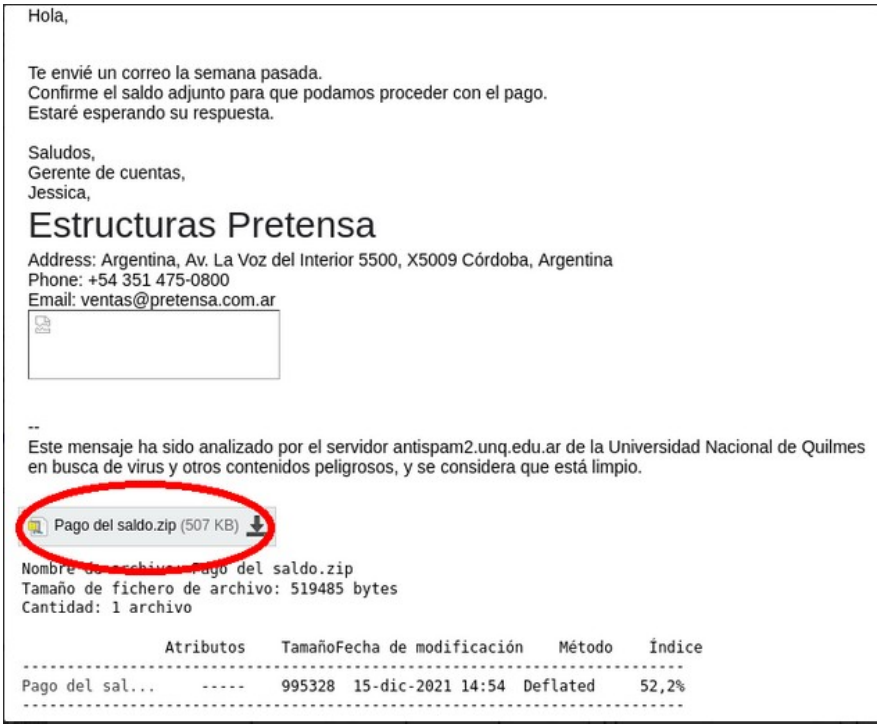
Virus detectado



Hola,

Te envié un correo la semana pasada.
Confirme el saldo adjunto para que podamos proceder con el pago.
Estaré esperando su respuesta.

Saludos,
Gerente de cuentas,
Jessica,

Estructuras Pretensa

Address: Argentina, Av. La Voz del Interior 5500, X5009 Córdoba, Argentina
Phone: +54 351 475-0800
Email: ventas@pretensa.com.ar

--
Este mensaje ha sido analizado por el servidor antispam2.unq.edu.ar de la Universidad Nacional de Quilmes en busca de virus y otros contenidos peligrosos, y se considera que está limpio.

Pago del saldo.zip (507 KB)

Nombre de archivo: Pago del saldo.zip
Tamaño de fichero de archivo: 519485 bytes
Cantidad: 1 archivo

	Atributos	Tamaño	Fecha de modificación	Método	Índice
Pago del sal...	-----	995328	15-dic-2021 14:54	Deflated	52,2%

La imagen muestra un ejemplo de correo electrónico engañoso que simula una comunicación comercial legítima para inducir a la persona destinataria a abrir un archivo adjunto. El mensaje utiliza un tono breve y aparentemente profesional, hace referencia a un supuesto pago pendiente y adjunta un archivo comprimido (`.zip`) que representa el principal vector de infección.

Este tipo de correos suele aprovechar la confianza en relaciones laborales o comerciales previas y puede incluir firmas empresariales falsas, direcciones reales o textos que aparentan haber sido analizados por sistemas de seguridad. Al abrir el archivo adjunto, el usuario puede ejecutar software malicioso destinado al robo de información, la instalación de malware o el acceso no autorizado al sistema.

Ante mensajes de estas características, se recomienda no abrir archivos adjuntos inesperados, verificar siempre la legitimidad del remitente por canales alternativos y reportar el correo como sospechoso a protege@unq.edu.ar