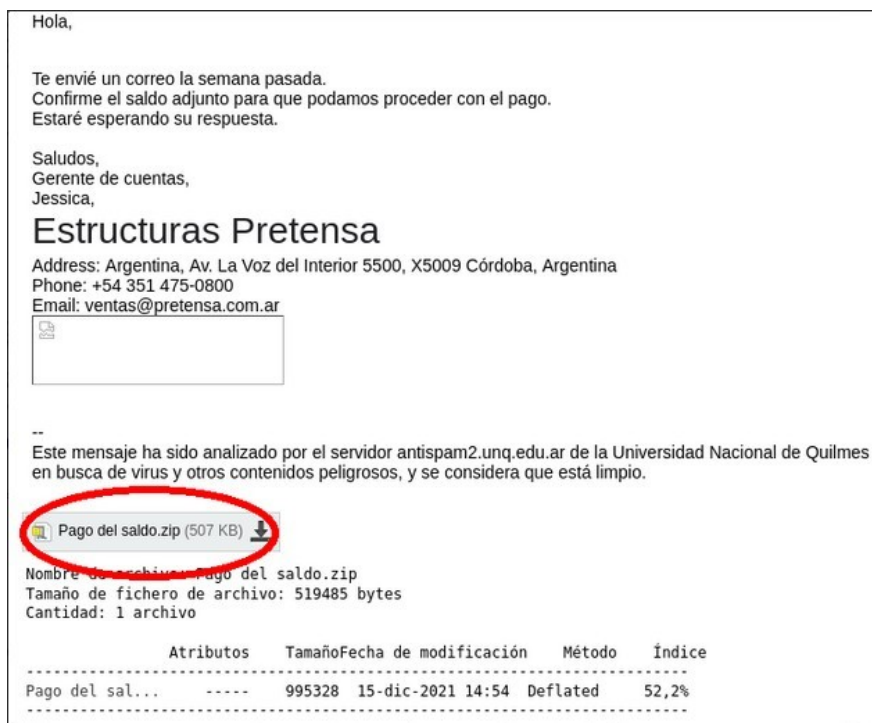


Virus detectado



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