# El propietario de MonsterCloud ha sido acusado de facturar más de 19 millones de dólares mientras pagaba de forma secreta rescates para descifrar datos

El Departamento de Justicia de Estados Unidos (DoJ) anunció el miércoles la presentación de cargos contra un ciudadano estadounidense e israelí de 50 años, quien presuntamente habría defraudado a víctimas de ransomware al pagar en secreto a los atacantes para conseguir herramientas de descifrado, mientras aseguraba que utilizaba soluciones propias para recuperar los datos.

Zohar Pinhasi (también conocido como Zack Silver y Zack Green) enfrenta dos cargos por fraude electrónico y uno por conspiración para cometer fraude electrónico. De ser declarado culpable, podría recibir una condena de hasta 20 años de prisión por cada cargo.

*"Al afirmar falsamente que podía descifrar ransomware sin pagar a los extorsionadores, el acusado volvió a convertir a sus propios clientes en víctimas, al mismo tiempo que obtenía importantes ganancias para sí mismo"*, declaró Joseph Nocella Jr., fiscal federal para el Distrito Este de Nueva York.

Pinhasi, propietario y operador de una empresa de Florida llamada MonsterCloud, presuntamente habría proporcionado información engañosa a personas afectadas por ataques de ransomware. Les recomendaba no pagar las exigencias de los atacantes y afirmaba contar con *"herramientas propietarias"* y *"técnicas avanzadas de descifrado"* capaces de recuperar los archivos afectados sin acceder a las demandas económicas de los ciberdelincuentes.

En su sitio web, MonsterCloud asegura emplear *"técnicas avanzadas de descifrado y tecnología de última generación"* para recuperar información. En un apartado titulado *"¿Debo pagar el rescate?"*, la compañía señala: *"Pagar un rescate a los ciberdelincuentes no garantiza un resultado favorable. De hecho, únicamente contribuye a incentivar y recompensar su comportamiento ilegal"*.

En una sección de preguntas y respuestas publicada en su página, MonsterCloud también respondía a la pregunta *"¿Pagan rescates en nombre de sus clientes para recuperar sus datos?"*. La empresa afirmaba: *"Aunque recomendamos firmemente que ustedes mismos no paguen rescates, contamos con amplia experiencia trabajando con responsables de ataques*

*de ransomware y, en ocasiones, recurrimos a otros métodos para solucionar el incidente de ransomware de nuestros clientes. Todos los términos se especifican en nuestro contrato de servicio"*.

Sin embargo, según la acusación, la compañía no disponía de herramientas especializadas capaces de descifrar los datos. En lugar de ello, Pinhasi habría contactado directamente con los ciberdelincuentes y les habría pagado para conseguir un programa de descifrado que permitiera recuperar la información.

Presuntamente, Pinhasi cobraba a los clientes de MonsterCloud cantidades *"considerablemente superiores"* al monto del rescate que pagaba de manera clandestina a los atacantes. En un caso ocurrido en agosto de 2023, el acusado habría entregado aproximadamente 8.200 dólares a un actor de amenazas y posteriormente habría facturado al cliente cerca de 150.000 dólares.

En otro incidente, ocurrido aproximadamente en octubre de 2021, Pinhasi habría efectuado un pago de rescate de unos 236.000 dólares y cobrado al cliente alrededor de 380.000 dólares. En total, se le acusa de haber facturado más de 19 millones de dólares a sus clientes y de haber destinado más de 8 millones de dólares al pago de rescates.

*"Según se alega, Zohar Pinhasi afirmaba solucionar ataques de ransomware sin llegar a eliminar la amenaza subyacente"*, señaló James C. Barnacle Jr., director adjunto de la Oficina Federal de Investigación de Estados Unidos (FBI). *"En cambio, convirtió la crisis de las víctimas en una fuente de ganancias personales. Este tipo de engaño es inaceptable"*.