LITORALPRESS

Fecha: 16-11-2024
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: Hackean información sensible sobre alumnos de la Universidad Federico Santa María

Pág. : 4
Cm2: 539,7
VPE: $ 2.967.995

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

El ataque fue el 24 de octubre y diez días después se publicó la información.

MOISÉS MUÑOZ

Datos privados y académicos de estudiantes de pre y post grado, y morosos de Crédito Universitario

Hackean información sensible sobre alumnos de la Universidad Federico Santa María

Esto podría ser aprovechado por otros atacantes para extorsionar y acceder a las claves de diferentes cuentas de las víctimas.

JORGE NÚÑEZ

La preocupación cunde en la Universidad Técnica Federico Santa María, tras hacerse público el ciberataque de RamsonHub, en que la banda de hackers accedió ilegalmente a unos 46 gigabytes de información sensible, tanto para la propia casa de estudios, como para sus trabajadores, alumnos y profesores.

Este viernes así lo reconoció la institución a través de un escueto comunicado. "El 24 de octubre se registró un incidente de seguridad informática, el cual fue detenido a tiempo gracias a los protocolos establecidos para estos casos, generando un impacto controlado en nuestros servicios".

Sin embargo no todos piensan lo mismo. Según reporta el portal fastcheck.cl, tras esperar diez días, los hackers publicaron en su sitio de la dark web o red oscura, unos 46 gigabytes de archivos.

Entre la información revelada, se cuentan varias listas en Excel con nombres, rut y carreras de cientos de alumnos de pre o post grado; además de información de carácter privado, como sus correos electrónicos y números telefónicos. A ello se suman parte de la base de datos del Centro de Alumnos y un listado con más de 2.700 ex alumnos que se encuentran en mora con el Fondo Solidario de Crédito Universitario.

Negociado oscuro

Aunque aclara que sin una investigación policial, "es prácticamente imposible determinar los motivos de este ataque", Alejandro Reid, académico de la Facultad de Comunicación de la Universidad de los Andes, postula que "probablemente los hackers intentaron negociar el rescate de los datos y al no llegar a acuerdo los publicaron en la Dark Web".De paso, aprovecha de explicar que, "la dark web es una parte pequeña de la deep web. La deep web es un área de Internet que no puede ser indexada y por lo tanto tampoco se puede rastrear a sus usuarios, ni desde donde vienen los datos. Además es entre 400 y 500 veces mas grande que la web normal o surface web, por lo que hay que usar navegadores seguros, también llamados onion browsers, por las múltiples capas de protección que tienen". Eso sí, navegar en la dark web es peligroso, ya que se asocia con actividades ilegales, como comercio de drogas, armas, pornografía y datos robados.En este último punto se detiene Fernando Lagos, gerente de Nivel 4 Cybersecurity, quien destaca estos ataques no solo se han vuelto más comunes, sino que incluso van más allá del cobro de rescate por la información. "Una vez que estos grupos organizados infectan sistemas y piden recompensas en criptomonedas a cambio de una clave que permita recuperar la información secuestrada, viene una segunda extorsión, en que piden dinero a cambio de no publicar la información, que puede ser aprovechada por otros atacantes, por terceros que la utilizan para extorsionar y acceder a las claves de diferentes cuentas de las víctimas", asegura el especialista.Tan rápido está creciendo el negociado de información robada en la deep web, que es posible encontrar hackers que venden el pack de ataque como servicio. "Es como que te vendieran el kit listo para hacer portonazos", asegura.Para acceder a sus víctimas, el modus operandi de estos grupos parte por la compra de credenciales en la deep web, pues con ellas acceden a los sistemas informáticos de sus víctimas. "Entonces pagan USD 5000 por una clave, pero terminan ganando mucho más cuando cobran el rescate de la información robada", finaliza.