

Grupo internacional hackea datos de docentes y alumnos de la USM

Ransom Hub opera con un ransomware - secuestro de datos - que restringe acceso a archivos del sistema operativo infectado. Publicaron información privada, lista de deudores y correos.

Mirian Mondaca Herrera
 mirian.mondaca@estrellavalpo.cl

Cerca de 46 gigabytes de información con datos personales de alumnos, profesores y correos electrónicos quedaron expuestos públicamente en el ciberespacio durante los últimos días, a raíz del hackeo del cual fue víctima la Universidad Santa María (USM) de Valparaíso. El grupo internacional Ransom Hub se adjudicó el ataque cuando a principios de noviembre, según consignó el medio electrónico Fast Check, anunció que había robado y publicaría información obtenida de la mencionada casa de estudios porteña. Diez días después, finalmente la información fue liberada.

Entre los archivos filtrados existen listas en formato Excel con información privada y de contacto de alumnos, centros de estudiantes y docentes. También el grupo expuso correos de la Mesa de Servicios de la universidad, la cual es parte del Departamento de Tecnologías de la Información y que gestiona requerimientos como cambio de contraseñas de los correos institucionales.



EN TOTAL, FUERON CERCA DE 46 GIGABYTES DE INFORMACIÓN EXTRAÍDA DE LA UNIVERSIDAD.

les. De igual forma se ventilaron mapas de las sedes de la USM y fotos personales de un funcionario.

Asimismo, se publicó un archivo con una lista con los deudores del Fondo Solidario de Crédito Universitario (FSCU), en el cual figura el rut, nombre, correo y fecha de inicio del cobro. Además, fueron vulnerados varios archivos Excel con los rut, sede, carrera, nombres y año de ingreso de los

alumnos matriculados de pregrado y cursando máster, así como un listado especial con estudiantes que integran el Centro de Alumnos de distintas sedes de la universidad, donde hasta se incluye el número de celular.

La Estrella pudo verificar además que en la web existen indicios de esta filtración de datos y que el mencionado grupo de alcance internacional ha efectuado ciberata-

ques a distintos organismos e instituciones del orbe. De hecho, durante la tarde de ayer se conoció que se añadió a su listado de víctimas el gobierno de México, al hackear datos de la Consejería Jurídica del Poder Ejecutivo Federal (CJEF). En ese caso, accedieron a contratos y datos personales de funcionarios.

La agrupación es considerada como una de las más activas y peligrosas

en en el panorama global, especialmente en Latinoamérica. El modo de operar es a través de un ransomware, o secuestro de datos en español, que es un tipo de software dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y generalmente pide un rescate para quitar esa restricción.

Consultados sobre el hackeo que sufrieron, desde la USM confirmaron la situación, mediante una escueta declaración, en la cual calificaron lo sucedido como un "incidente de seguridad informática" ocurrido el 24 de octubre pasado, y que "fue detenido a tiempo" a raíz de los protocolos establecidos para estos casos, "generando un impacto controlado en nuestros servicios".

"Al igual que muchas instituciones, nuestra universidad se mantiene atenta a este tipo de amenazas, las cuales son detectadas de manera oportuna por nuestros sistemas de ciberseguridad, los que constantemente se optimizan para proteger los datos de nuestra comunidad universitaria", acotaron en la breve declaración. ☺