LITORALPRESS

Fecha: 16-11-2024
Medio: El Mercurio de Valparaíso
Supl. : El Mercurio de Valparaiso
Tipo: Noticia general
Título: Universidad Santa María sufrió ataque de grupo de hackers internacionales

Pág. : 4
Cm2: 571,4
VPE: $ 1.374.295

Tiraje: 11.000
Lectoría: 33.000
Favorabilidad: No Definida

# Universidad Santa María sufrió ataque de grupo de *hackers* internacionales

**VALPARAÍSO.** *Aseguran que lograron controlarlo a tiempo; sin embargo, medio especializado dio cuenta que piratas informáticos accedieron a datos sensibles de la casa de estudios y publicaron información extraída.*

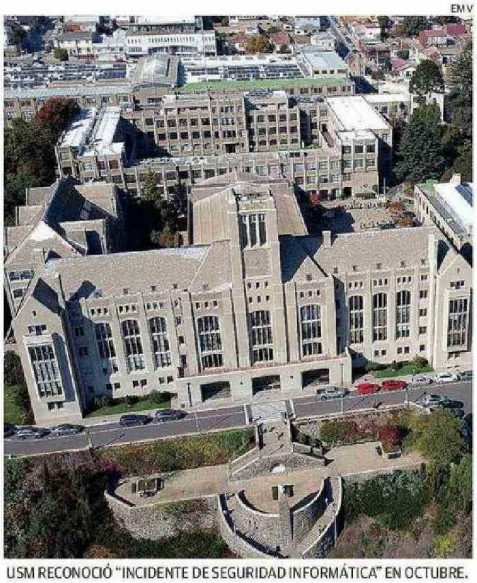
Cristián Rojas M.
*cristian.rojas@mercuriovalpo.cl*

La Universidad Técnica Federico Santa María (USM), de reconocido prestigio en materia de tecnología e informática, sufrió el ataque de un grupo de *hackers* internacionales denominado Ransom Hub, información dada a conocer en su cuenta de X por el investigador independiente en ciberseguridad @chum1ng0.

Al respecto, desde la USM señalaron a este Diario que "el 24 de octubre nuestra casa de estudios 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".

Aseguraron que "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. Es importante destacar también que nuestra casa de estudios entrega continuamente recomendaciones sobre ciberseguridad a sus profesores, estudiantes y funcionarios, a través de los canales institucionales".

Sin embargo, desde la casa de estudios no se refirieron a un episodio que se habría registrado a principios de este mes y que fue comentado por especialistas en la materia.



EMV

USM RECONOCIÓ "INCIDENTE DE SEGURIDAD INFORMÁTICA" EN OCTUBRE.

## PUBLICAN DATOS SENSIBLES

Según publicó la página digital de periodismo Fast Check CL, el grupo *hacker* Ransom Hub publicó en su sitio -en la *dark web*- 46 gigabytes de información extraída de la USM. Entre los archivos figuran listas con datos personales de alumnos y profesores, además de correos de la Mesa de Servicios de la universidad.

Entre los archivos se contarían listas en Excel con información privada y de contacto de alumnos, centros de estudiantes y profesores.

Otro de los contenidos es una lista con los deudores del Fondo Solidario. Compendio de más de 2.700 alumnos en mora por el FSCU, en que figura su rut, nombre, correo y fecha de inicio de cobro.

También se publicaron archivos Excel con rut, sede, carrera, nombres y año de ingreso de los alumnos, desde matriculados, al día y cursando magíster.

## COBRAN POR RESCATE

El director de la Escuela de Ingeniería de la Universidad Andrés Bello Sede Viña del Mar, David Ruete, cuya área de investigación son las redes de comunicaciones y la seguridad en redes de computadores y la inteligencia artificial, explicó que "el *ransomware* es un tipo de *software* malicioso que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción. Los atacantes suelen cifrar los archivos de la víctima, haciéndolos inaccesibles, y exigen un pago para proporcionar la clave de descifrado para restaurar el acceso".

Precisó que "la USM fue atacada por el grupo RansomHub, conocido por operar bajo el modelo de *ransomware* como servicio (RaaS) y emplear tácticas de doble extorsión, cifrando los datos de las víctimas y amenazando con publicarlos si no se paga el rescate. Según la clasificación proporcionada anteriormente, este ataque corresponde a un *ransomware* de cifrado que utiliza tácticas de doble extorsión y opera bajo el modelo de *ransomware* como servicio (RaaS)".

Por otro lado, Ruete advirtió que "las autoridades y expertos en ciberseguridad desaconsejan pagar el rescate, ya que no garantiza la recuperación de los datos y financia actividades delictivas".

Por su parte, Sebastián Berríos, ingeniero civil en Computación e Informática y docente de Ciberseguridad en la PUCV, puntualizó que "a nivel internacional, uno de los casos de mayor interés es el de Colonial Pipeline, en Estados Unidos, donde el grupo DarkSide provoca un cierre temporal de la principal red de oleoductos del país, es decir, un ataque a la infraestructura crítica. Hoy en día los ciberdelincuentes están atacando constantemente la infraestructura crítica, porque se dieron cuenta que podían obtener muchos beneficios económicos. Este caso llevó a un rescate de 4,4 millones de dólares, con lo cual fue uno de los ataques más importantes en el área de Estados Unidos".

## MEDIDAS PREVENTIVAS

Para prevenir este tipo de ataques, agregó Berríos, "todo parte por la educación, hoy en día es fundamental, el 90% de los ataques de ciberseguridad son por fallas humanas. Podemos implementar tremenda infraestructura en ciberseguridad, pero si no generamos una educación, una capacitación y una validación, para saber si realmente nuestros trabajadores están capacitándose y están entendiendo lo que están haciendo, o si siguen apretando ese correo o bajando archivos que no corresponden, obviamente siguen vulnerando la infraestructura de la empresa".

"Si lo vemos a nivel de infraestructura, tenemos que trabajar en las actualizaciones regulares, ver temas de parches, respuestas a incidentes, copias de seguridad y recuperación. Siempre he dicho que la posibilidad de que todos sufran un ataque de ciberseguridad es súper viable", advirtió Berríos, cuya área de investigación es la identificación y clasificación de *malwares* con utilización de inteligencia artificial, la integración de ciberseguridad en computación cuántica y privacidad de datos.

En el Congreso, en tanto, uno de los principales impulsores de la ciberseguridad es el senador por la Región de Valparaíso Kenneth Pugh (indep.-RN), quien señaló que para prevenir dichos ataques "lo principal es desarrollar sistemas que sean ciberseguros por diseño".

"Otro tema relevante es mantener los sistemas actualizados y estar constantemente preocupados de conocer las vulnerabilidades que se publican e instalar los parches de *software* que permiten reducir el riesgo de ataque", agregó el parlamentario.

## TODOS SON VULNERABLES

Pugh advirtió que "no existe ningún tipo de sistema que sea invulnerable, ataques de este tipo se ven en todas partes del mundo, no solamente en Chile. Múltiples universidades de prestigio a nivel mundial han sido atacadas, sistemas estatales de países de la talla del Reino Unido o incluso Estados Unidos".

Frente a ello, subrayó que "en ciberseguridad la colaboración es la piedra angular, pues no existe institución que sea inmune a un ataque. El trabajo de colaboración se reflejará mejor al entrar en servicio la nueva Agencia Nacional de Ciberseguridad, que dispondrá de un nuevo CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) nacional, que siempre estará informando de vulnerabilidades y sus actualizaciones, junto a ataques en progreso a sistemas críticos y vitales".

Sobre si es posible perseguir legalmente desde Chile a *hackers* internacionales, el senador planteó que "en la medida que se detecten sus orígenes, se puede, gracias a que nuestro país está suscrito al Convenio de Budapest, que permite la persecución transfronteriza del cibercrimen, con 68 Estados que son parte del acuerdo. El desafío es determinar la atribución del ataque, lo que requiere de gran especialización de las brigadas de Cibercrimen de la PDI y el traspaso de la evidencia digital entre fiscalías".

> **"Ciberdelincuentes están atacando la infraestructura crítica, porque se dieron cuenta que podían obtener muchos beneficios económicos".**
>
> David Ruete
> Académico UNAB Viña del Mar

> **"Múltiples universidades de prestigio a nivel mundial han sido atacadas, sistemas estatales de países de la talla del Reino Unido o incluso EE.UU.".**
>
> Kenneth Pugh
> Senador

> **"Tenemos que trabajar en las actualizaciones regulares, ver temas de parches, respuestas a incidentes, copias de seguridad y recuperación".**
>
> Sebastián Berríos
> Académico PUCV