

Alerta de seguridad cibernética	8FFR21-01011-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre de 2021

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno) ha identificado la activación de una página fraudulenta que suplanta al Banco de Chile, la que podría servir para robar credenciales de sus usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

## Indicadores de compromiso

### URL sitio falso

[https://www.soporte-bchile.cl.bonafidelabs\[.\]in/1631539133/bcochile-web/persona/login/index.html/login](https://www.soporte-bchile.cl.bonafidelabs[.]in/1631539133/bcochile-web/persona/login/index.html/login)

### Certificado Digital

Fecha Válido	12-09-2021
Fecha Término	12-12-2021
Emitido	cPanel, Inc. Certification Authority

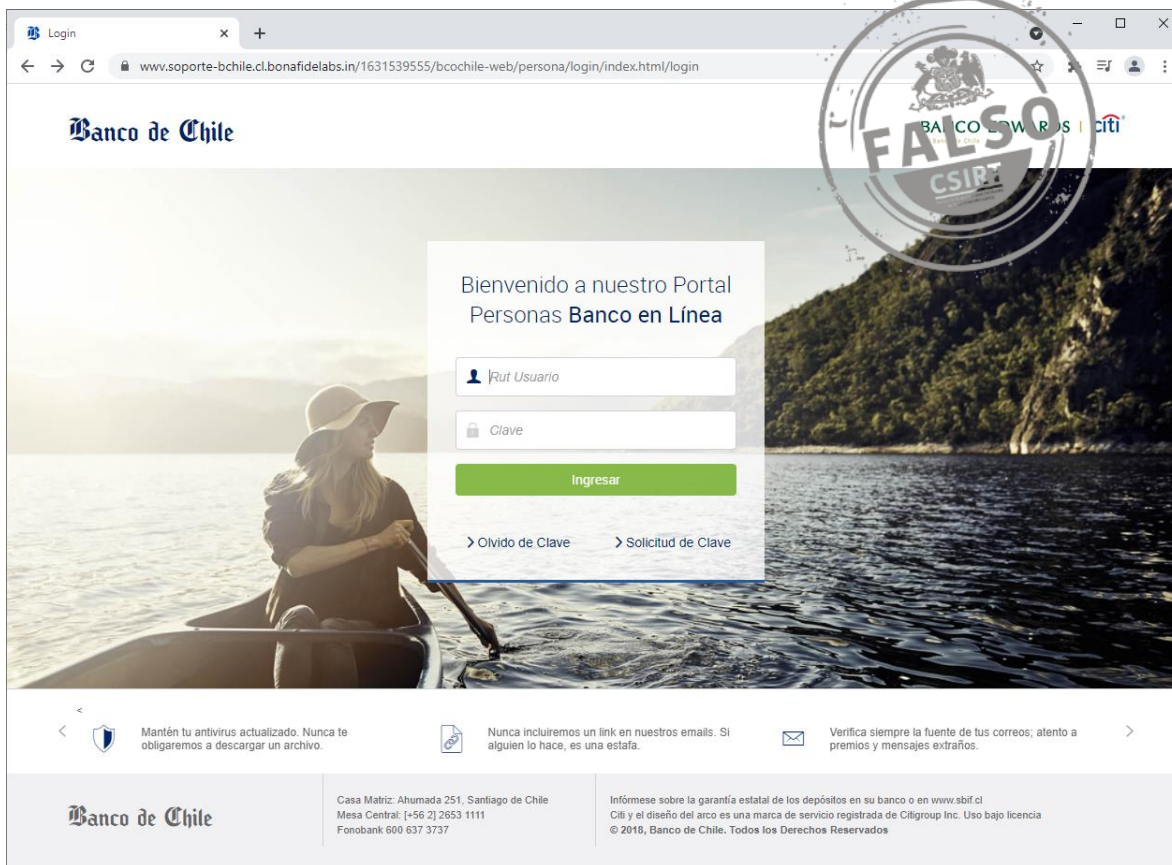
### Datos Alojamiento

IP	[198.136.51.114]
Número de Sistema Autónomo (AS)	33182
Etiqueta del Sistema Autónomo	DIMENOC
País	US
Registrador	ARIN

### Datos del Dominio

Nombre de Dominio	bonafidelabs.in
Creado	05-10-2020
Expira	05-010-2021
Información del Registrador	ZNet Technologies Private Limited
ID IANA	1628
Correo Electrónico	<a href="mailto:abuse@namecheap.com">abuse@namecheap.com</a>
Servidores DNS	ns1.sysbitech.com ns2.sysbitech.com

## Imagen del sitio



The image shows a screenshot of the Banco de Chile login page. The browser address bar displays the URL: [www.soporte-bchile.cl/bonafidelabs.in/1631539555/bcochile-web/persona/login/index.html/login](http://www.soporte-bchile.cl/bonafidelabs.in/1631539555/bcochile-web/persona/login/index.html/login). The page features the Banco de Chile logo and a large background image of a person in a boat on a lake. A central white box contains the text "Bienvenido a nuestro Portal Personas Banco en Línea" and a login form with fields for "Rut Usuario" and "Clave", an "Ingresar" button, and links for "Olvido de Clave" and "Solicitud de Clave". A large circular watermark with the word "FALSO" and the CSIRT logo is overlaid on the right side of the page. At the bottom, there are three security notices: "Mantén tu antivirus actualizado. Nunca te obligaremos a descargar un archivo.", "Nunca incluiremos un link en nuestros emails. Si alguien lo hace, es una estafa.", and "Verifica siempre la fuente de tus correos; atento a premios y mensajes extraños." The footer includes the Banco de Chile logo, contact information for the main office, and a copyright notice for 2018.

## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.