

|                                 |  |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR20-0088-01                         |
| Clase de alerta                 | Fraude                                 |
| Tipo de incidente               | Falsificación de Registros o Identidad |
| Nivel de riesgo                 | Alto                                   |
| TLP                             | Blanco                                 |
| Fecha de lanzamiento original   | 11 de Julio de 2020                    |
| Última revisión                 | 11 de Julio de 2020                    |

## 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 (CSIRT), ha identificado la activación de un portal fraudulento asociado a un dominio que suplanta el sitio web oficial de **Banco Estado**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

## Indicadores de compromiso

### Urls sitio falso:

www-bancoestado[.]cl[.]sahifa-news[.]com/pagina/imagenes/comun2008/banca-en-linea-personas[.]html

### Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

### Certificado Digital

Fecha Valido : miércoles, 8 de julio de 2020 20:00:00  
Fecha Termino : miércoles, 7 de octubre de 2020 19:59:59  
Emitido : CN = cPanel, Inc. Certification Authority

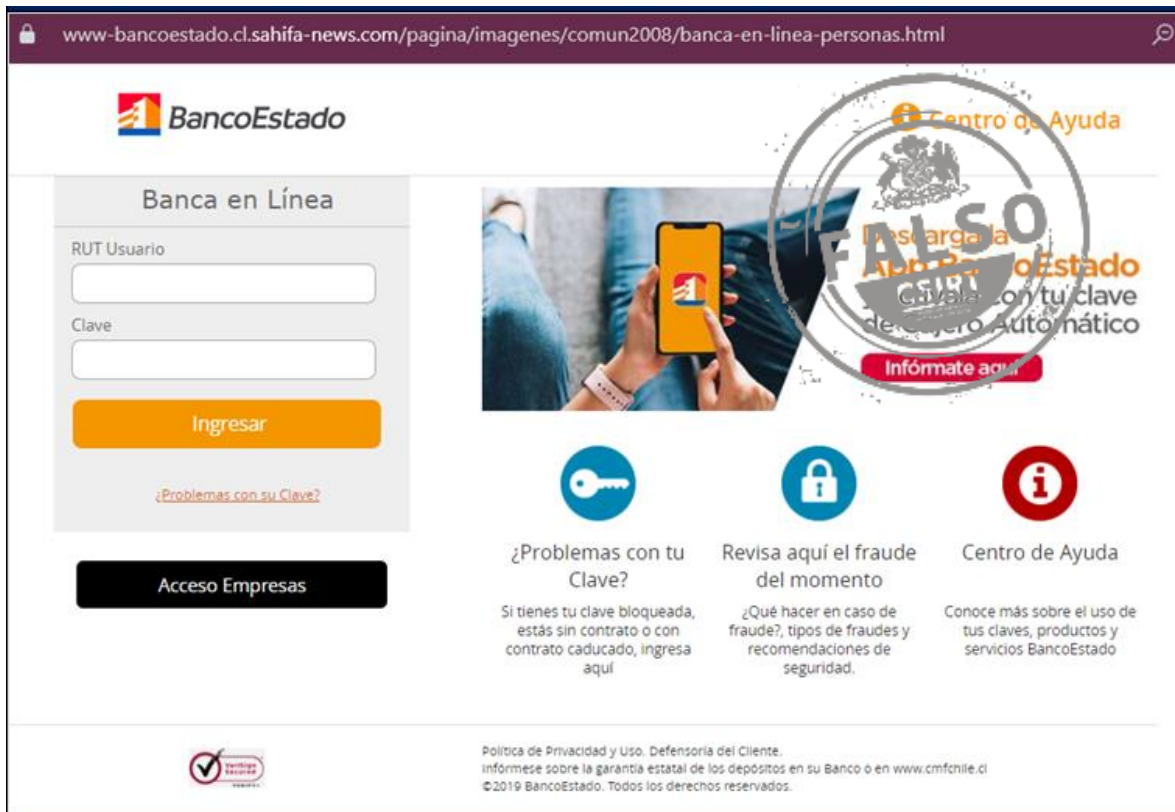
### Datos Alojamiento

IP : 23[.]235[.]221[.]30  
Número de sistema autónomo (AS) : 22611  
Etiqueta del sistema autónomo : InMotion Hosting, Inc.  
País : Estados Unidos  
Registrador : ARIN

### Datos del Dominio

Nombre de dominio : sahifa-news.com  
Estado del dominio : Activo  
Creado : 2018-01-21  
Expira : 2021-01-21  
Información del registrador : GoDaddy.com, LLC  
ID IANA : 146  
Correo electrónico : -  
Servidores de nombres : ns1.muchohost.com  
ns2.muchohost.com

## Imagen del sitio



The screenshot shows the BancoEstado website interface. At the top, the URL is [www-bancoestado.cl.sahifa-news.com/pagina/imagenes/comun2008/banca-en-linea-personas.html](http://www-bancoestado.cl.sahifa-news.com/pagina/imagenes/comun2008/banca-en-linea-personas.html). The BancoEstado logo is visible. The main content area is titled "Banca en Línea" and contains a login form with fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "¿Problemas con su Clave?". Below the login form is a button for "Acceso Empresas". To the right, there is a large graphic with the word "FALSO" in a large, stylized font, overlaid on a background image of a person using a smartphone. The graphic also includes the text "¿Carga la App de BancoEstado con tu clave de acceso Automático" and "Infórmate aquí". Below this graphic are three columns of information: 1. "¿Problemas con tu Clave?" with a key icon, explaining that if the key is blocked, expired, or the contract is expired, the user should log in. 2. "Revisa aquí el fraude del momento" with a padlock icon, providing information on what to do in case of fraud, types of frauds, and security recommendations. 3. "Centro de Ayuda" with an information icon, directing users to learn more about key usage, products, and services. At the bottom of the page, there is a "Política de Privacidad y Uso. Defensoría del Cliente" link, information about the state deposit guarantee, and a copyright notice for 2019 BancoEstado.

## 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.