

Alerta de seguridad cibernética	8FFR20-00661-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Agosto de 2020
Última revisión	27 de Agosto 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 afecta 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 aludida.

## Indicadores de compromiso

### Urls sitio falso:

bancoestado-bancaporinternet[.]link/inicio/imagenes/comun2008/banca-en-linea-personas[.]html

### Redirector:

hxxps://bit[.]ly/3hoJshH

### Body SHA-256

53c16aca165fb6b49e976c397832e560aa733c484b2b891d8623cd1df7295bec

### Certificado Digital

Fecha Valido : domingo, 23 de agosto de 2020 20:00:00  
Fecha Termino : martes, 24 de agosto de 2021 19:59:59  
Emitido : Sectigo Limited

### Datos Alojamiento

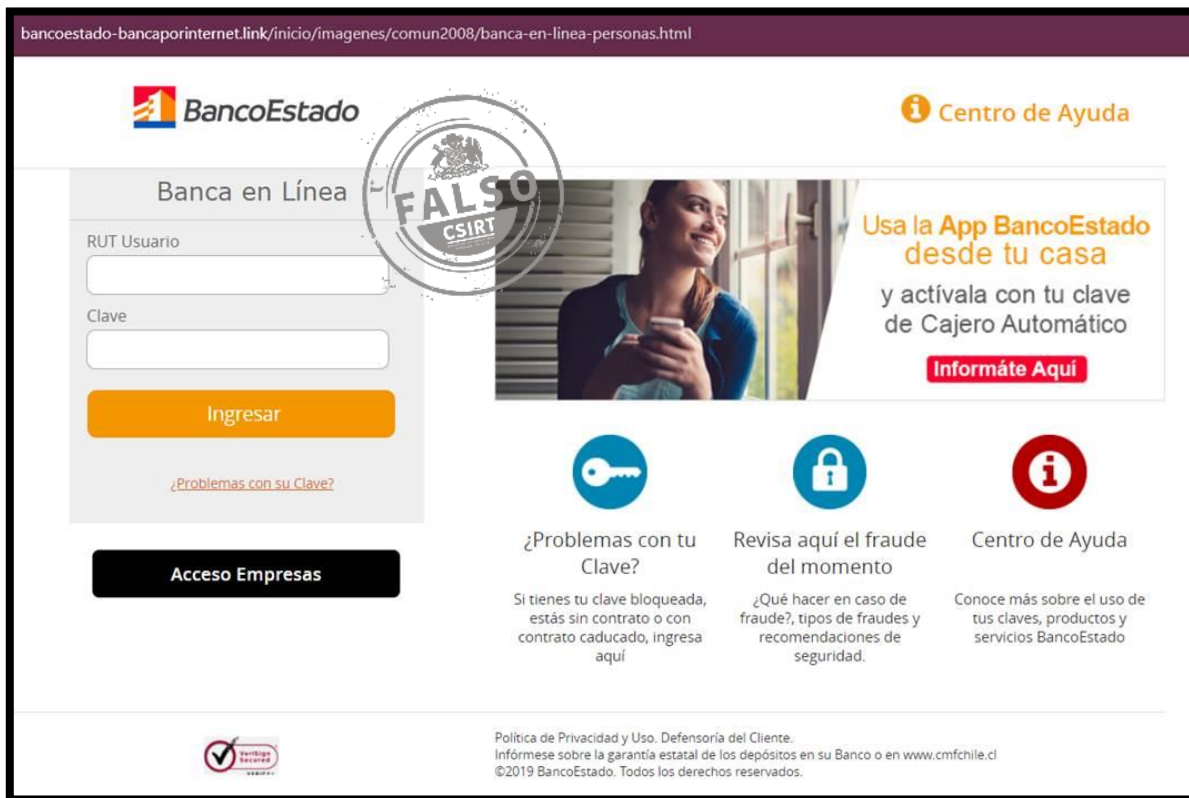
IP : 68[.]65[.]123[.]126  
Número de sistema autónomo (AS) : 22612  
Etiqueta del sistema autónomo : Namecheap, Inc  
País : Estados Unidos  
Registrador : ARIN

### Datos del Dominio

Nombre de dominio : bancoestado-bancaporinternet[.]link  
Estado del dominio : Activo  
Creado : 2020-08-24  
Expira : 2021-08-24  
Información del registrador : NAMECHEAP  
ID IANA : 1068  
Correo electrónico : No Encontrado  
Servidores de nombres : dns2[.]namecheaposting[.]com  
dns1[.]namecheaposting[.]com

## Imagen del sitio

bancoestado-bancaporinternet.link/inicio/imagenes/comun2008/banca-en-línea-personas.html



**BancoEstado**

**Banca en Línea**

RUT Usuario

Clave

**Ingresar**

[¿Problemas con su Clave?](#)

**Acceso Empresas**

**Centro de Ayuda**

**Usa la App BancoEstado desde tu casa**  
y actívala con tu clave de Cajero Automático  
**Informáte Aquí**

**¿Problemas con tu Clave?**  
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí

**Revisa aquí el fraude del momento**  
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.

**Centro de Ayuda**  
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

**Verifica Seguro**

Política de Privacidad y Uso. Defensoría del Cliente.  
Infórmese sobre la garantía estatal de los depósitos en su Banco o en [www.cmfchile.cl](http://www.cmfchile.cl)  
©2019 BancoEstado. Todos los derechos reservados.

## 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.