

Alerta de seguridad cibernética	8FFR20-00855-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Diciembre de 2020
Última revisión	22 de Diciembre 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 una página fraudulenta asociada al dominio .cl que intenta suplantar a Banco Estado que podría servir para robar credenciales de clientes de la entidad bancaria.

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

<http://bancoestadocredito.cl/bancoestado/pagina/imagenes/comun2008/banca-en-linea-personas.html>

Certificado Digital

Fecha Válido	No aplica
Fecha Término	No aplica
Emitido	No aplica

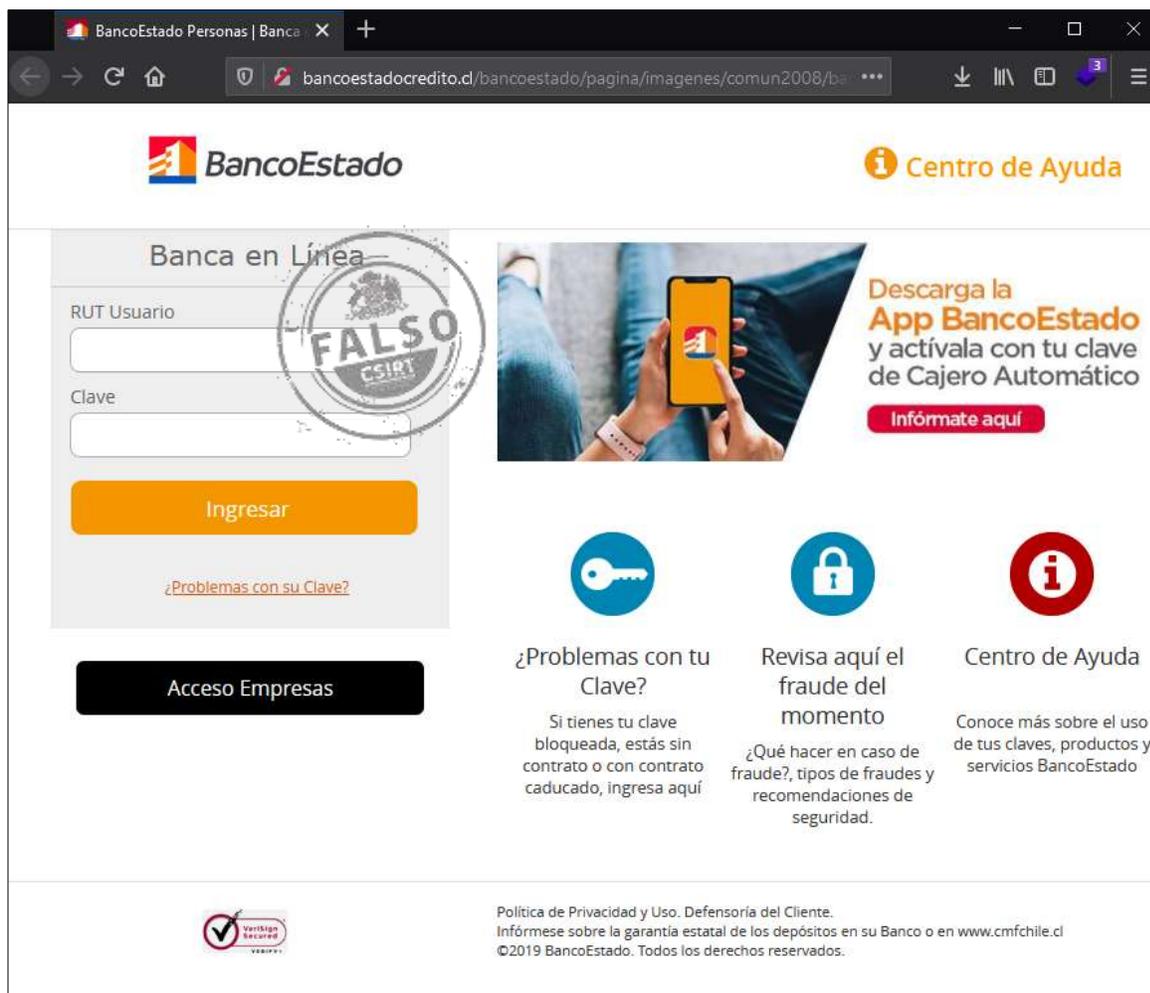
Datos Alojamiento

IP	186[.]64[.]118[.]235
Número de Sistema Autónomo (AS)	52368
Etiqueta del Sistema Autónomo	ZAM LTDA.
País	CL
Registrador	LACNIC

Datos del Dominio

Nombre de Dominio	bancoestadocredito.cl
Creado	15-12-2020
Expira	15-12-2021
Información del Registrador	Haulmer SpA
ID IANA	
Correo Electrónico	
Name Server	ns1.dnshosty.net ns2.dnshosty.net ns3.dnshosty.net

Imagen del sitio



BancoEstado Personas | Banca

bancoestadocredito.cl/bancoestado/pagina/imagenes/comun2008/ba...

BancoEstado Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas

Descarga la **App BancoEstado** y actívala con tu clave de Cajero Automático

Infórmate 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

Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en 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.