

Alerta de seguridad cibernética	8FFR20-00440-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de Junio de 2020
Última revisión	05 de Junio 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 bancaria aludida.

## Indicadores de compromiso

### Urls sitio falso:

hxxp://www.ban.estado-creditos[.]net

### Body SHA-256

7abc7066c6325f670480ae5d84cec1a49918533b8d8872c7a5650c9e33503942

### Certificado Digital

Fecha Valido	:	No presenta
Fecha Termino	:	No presenta
Emitido	:	No presenta

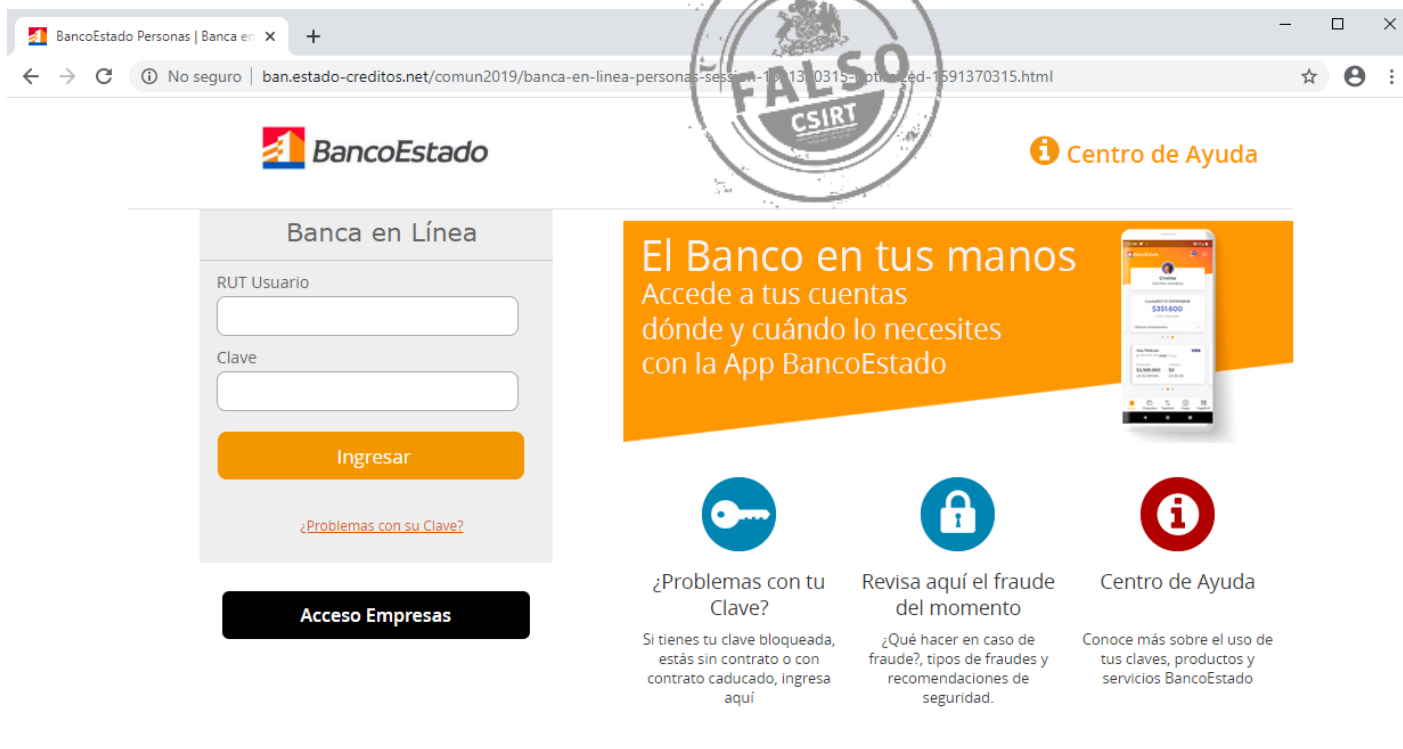
### Datos Alojamiento

Red	:	85.187.128.0/19
IP	:	85.187.132.184
Número de sistema autónomo (AS)	:	55293
Etiqueta del sistema autónomo	:	A2 Hosting, Inc
País	:	Estados Unidos
Registrador	:	ARIN

### Datos del Dominio

Nombre de dominio	:	ban.estado-creditos[.]net
Estado del dominio	:	clientTransferProhibited addPeriod
Creado	:	04 de junio de 2020
Actualizado	:	
Expira	:	06 de junio de 2021
Información del registrador	:	Namecheap Inc
ID IANA	:	1068
Correo electrónico	:	abuse@namecheap.com
Servidores de nombres	:	ns85187132169.a2dns.com ns8518713217.a2dns.com

## Imagen del sitio



The screenshot shows a web browser window with the address bar displaying "ban.estado-creditos.net/comun2019/banca-en-linea-personas-septiembre-13-2019-otro-med-1591370315.html". A large, semi-transparent watermark with the word "FALSO" and the CSIRT logo is overlaid on the page. The website content includes the BancoEstado logo, a "Centro de Ayuda" link, and a "Banca en Línea" login section with fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "¿Problemas con su Clave?". Below the login section is a "Acceso Empresas" button. To the right, a promotional banner for the "Banco en tus manos" app is displayed, along with three informational icons: a key for login issues, a padlock for fraud, and an information icon for the help center.

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.