

Alerta de seguridad cibernética	8FFR20-0085-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de Julio de 2020
Última revisión	10 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:

banco[.]acessoestado[.]com

### Body SHA-256

c71ecb9edc3b5deaefa6f68c6912f151c6ade8c883a6c5811d174025f848d510

### Certificado Digital

Fecha Valido : jueves, 9 de julio de 2020 01:19:48 p.m  
Fecha Termino : miércoles, 7 de octubre de 2020 02:19:48 p.m  
Emitido : Let's Encrypt Authority X3

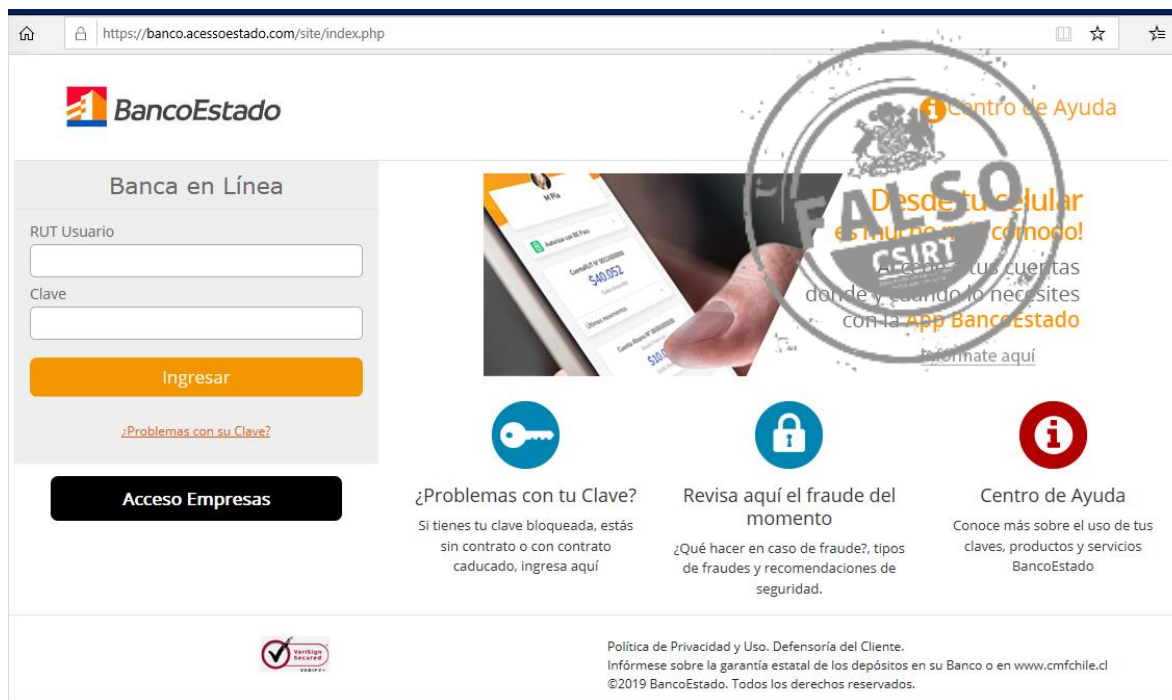
### Datos Alojamiento

IP : 195[.]189[.]96[.]36  
Número de sistema autónomo (AS) : 59642  
Etiqueta del sistema autónomo : UAB Cherry Servers  
País : LT  
Registrador : -

### Datos del Dominio

Nombre de dominio : banco[.]acessoestado[.]com  
Estado del dominio : Activo  
Creado : 2020-07-08 21:20:02  
Expira : 2021-07-08 21:20:01  
Información del registrador : Google LLC  
ID IANA : 895  
Correo electrónico : n1d7zkqoj2cv@contactprivacy[.]email  
Servidores de nombres : ns-cloud-d1[.]googledomains[.]com  
ns-cloud-d2[.]googledomains[.]com  
ns-cloud-d3[.]googledomains[.]com  
ns-cloud-d4[.]googledomains[.]com

## Imagen del sitio



The screenshot shows the BancoEstado website interface. At the top left is the BancoEstado logo. Below it is a 'Banca en Línea' section with a login form containing fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. To the right is a large banner for the mobile app with the text 'Desde tu celular es más cómodo!' and 'Accede a tus cuentas donde y cuando lo necesites con la App BancoEstado'. Below the banner are three service tiles: '¿Problemas con tu Clave?' (with a key icon), 'Revisa aquí el fraude del momento' (with a padlock icon), and 'Centro de Ayuda' (with an information icon). At the bottom, there is a 'Verifica Seguro' logo and a footer with the text: '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.