

Alerta de seguridad informática	8FFR-00010-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	31 de Julio de 2019
Última revisión	31 de Julio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones 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 a directamente a las entidades ni al sistema bancario, sino que son técnica 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 llamado a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de portales fraudulentos que suplantan el sitio web oficial del **BANCOESTADO.CL** con el objetivo de obtener las credenciales de potenciales víctimas. Algunos de los sitios incluso cuentan con certificados que les permiten tener el candado para brindar la sensación de seguridad a los usuarios que puedan ser víctimas del fraude.

Lo anterior constituye una falsificación de la marca institucional con fines de fraude hacia los usuarios y/o clientes de la entidad afectada.

Indicadores de Compromisos

URL's

http[:]//bncostado-cl[.]xyz
https[:]//bncostado[.]xyz/imagenes/comun2009/en-linea-personas[.]php
bncostado[.]xyz
bncostado-cl[.]xyz
http[:]//bncostado-cl[.]xyz/imagenes/comun2009/en-linea-personas[.]php

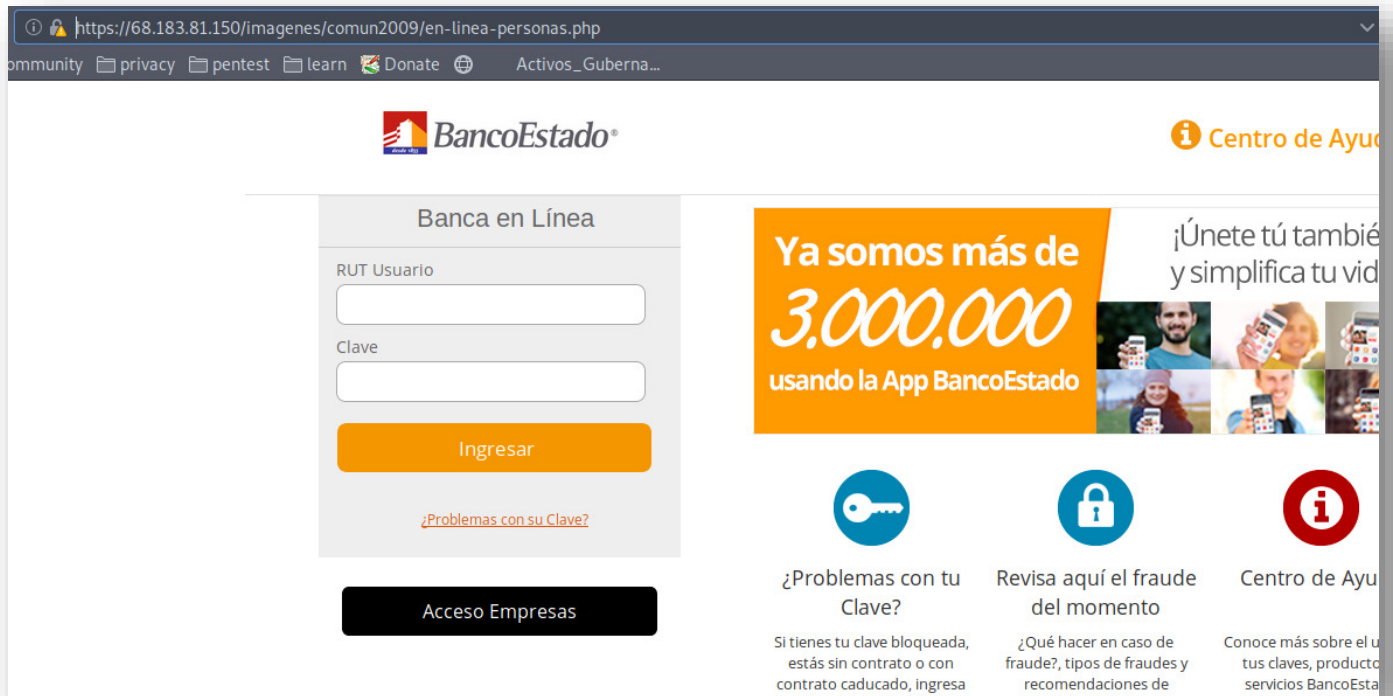
IP's

68.183.81.150
139.59.66.85

Localización en red

AS14061 DigitalOcean, LLC, geolocalizado en la India.
AS19817 DSL Extreme, geolocalizada en los EE.UU.

Ejemplo de Imagen de los sitios



The screenshot shows the BancoEstado website interface. At the top left is the BancoEstado logo. On the right, there is a 'Centro de Ayuda' (Help Center) link. The main content area is divided into two sections:

- Left Section (Banca en Línea):** A login form titled 'Banca en Línea' with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below this is a black button for 'Acceso Empresas'.
- Right Section (Promotional Banner):** An orange banner stating 'Ya somos más de 3.000.000 usando la App BancoEstado' with the text '¡Únete tú también y simplifica tu vida!'. Below the banner are three columns of information: a key icon for '¿Problemas con tu Clave?', a padlock icon for 'Revisa aquí el fraude del momento', and an information icon for 'Centro de Ayuda'.

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre la existencia del sitio, para que no ser víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido
- 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

Contactos



<https://www.csirt.gob.cl>



+ (562) 24863850



@CSIRTGOB



<https://www.linkedin.com/company/csirt-gob>