

Alerta de seguridad informática	8FFR-00012-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Agosto de 2019
Última revisión	09 de Agosto 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 un portal fraudulento que suplanta el sitio web oficial del BANCOESTADO.CL el que podría servir para robar credenciales de usuarios del banco.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL's

http[:]//bcoestadocl[.]com
http[:]//bcoestadocl[.]com/imagenes/comun2008/

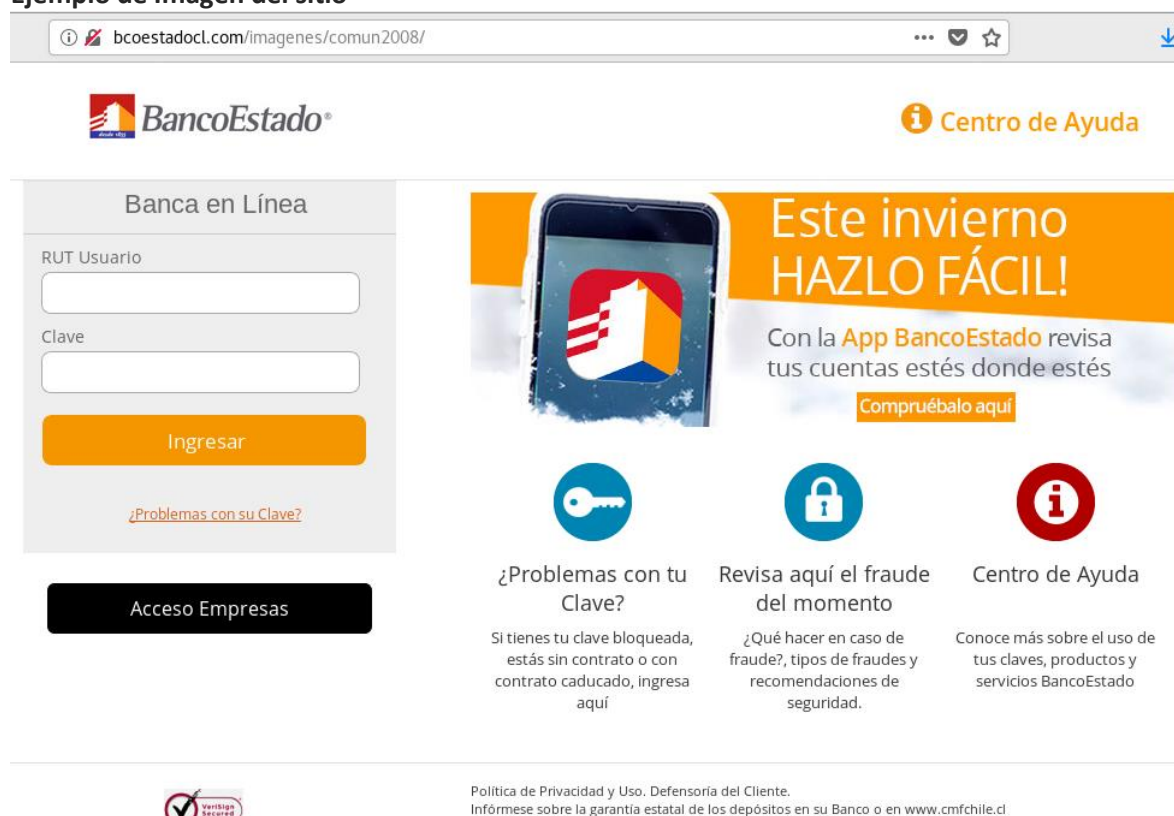
IP's

186.64.116.35

Localización en red

AS52368 ZAM LTDA

Ejemplo de Imagen del sitio



The screenshot shows the BancoEstado website interface. At the top left is the BancoEstado logo. To the right is a 'Centro de Ayuda' link. The main content area is divided into two sections. On the left is the 'Banca en Línea' login form, which includes fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is a 'Acceso Empresas' button. On the right is a promotional banner for the 'App BancoEstado' with the headline 'Este invierno HAZLO FÁCIL!' and the text 'Con la App BancoEstado revisa tus cuentas estés donde estés'. Below the banner are three icons: a key, a padlock, and an information icon. Each icon has a corresponding title and description: '¿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), and 'Centro de Ayuda' (Conoce más sobre el uso de tus claves, productos y servicios BancoEstado). At the bottom of the page, there is a 'Verifica Seguridad' logo and a link to the 'Política de Privacidad y Uso. Defensoría del Cliente.' with the text 'Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl'.

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