

Alerta de seguridad informática	8FFR-00062-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Septiembre de 2019
Última revisión	16 de Septiembre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias 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 una IP 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 Compromisos

URL's

https://terrium.cl/css/date/imagenes/comun2008/banca-en-linea-personas.html

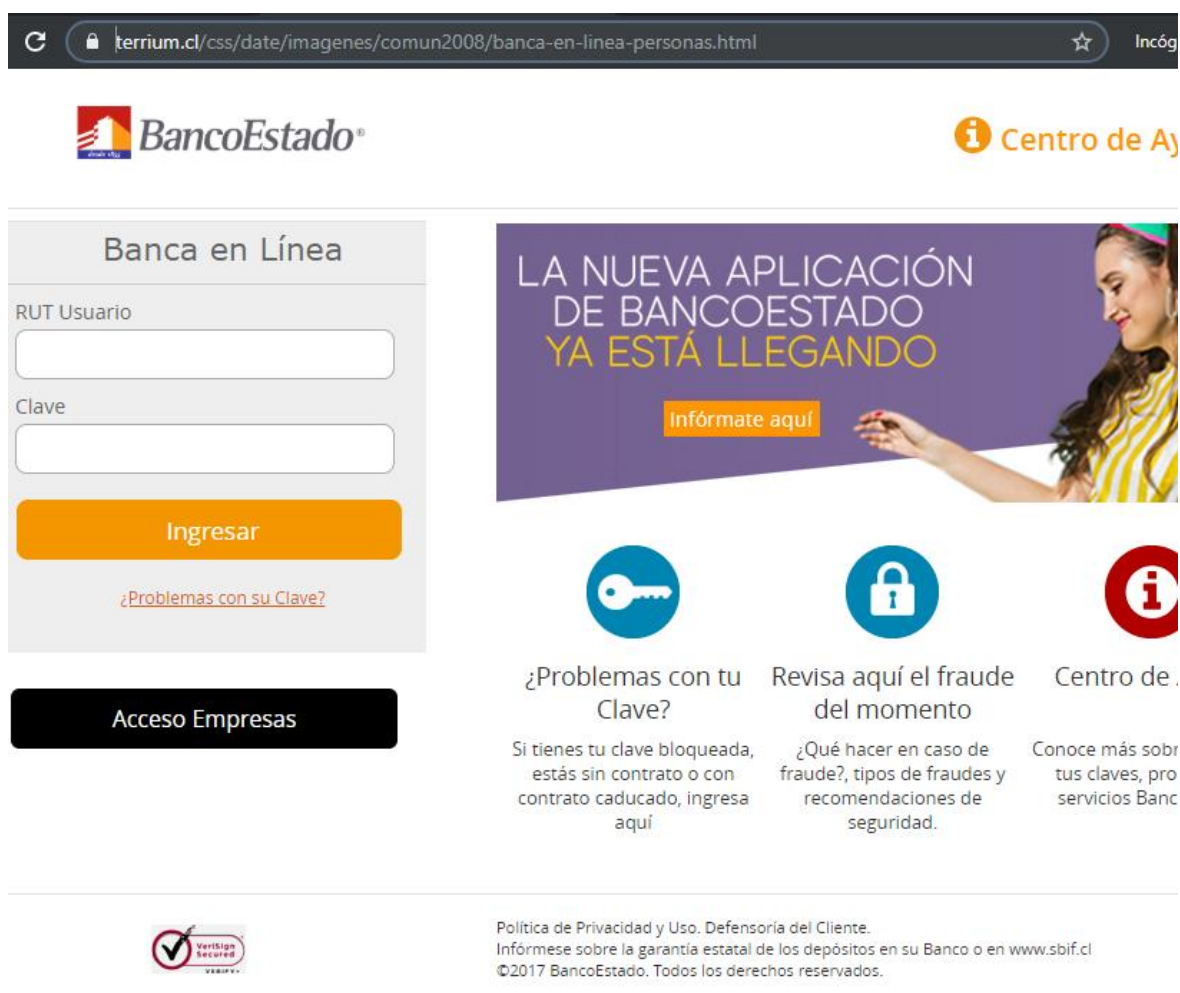
IP's

108.179.227.230

Localización

Houston, Texas, Estados Unidos

Ejemplo de Imagen del sitio



The screenshot shows the login page for BancoEstado's online banking. The browser address bar displays the URL: `terrium.cl/css/date/imagenes/comun2008/banca-en-linea-personas.html`. The page features the BancoEstado logo and a navigation menu with "Centro de Ay" (Help Center). The main content area is divided into two sections. On the left, there is a login form titled "Banca en Línea" with input fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "¿Problemas con su Clave?". Below the form is a button for "Acceso Empresas". On the right, there is a promotional banner for a new app: "LA NUEVA APLICACIÓN DE BANCOESTADO YA ESTÁ LLEGANDO" with an "Infórmate aquí" button. Below the banner are three service tiles: 1. "¿Problemas con tu Clave?" with a key icon, describing issues with blocked keys or expired contracts. 2. "Revisa aquí el fraude del momento" with a padlock icon, providing information on current fraud types and security recommendations. 3. "Centro de" with an information icon, offering more details about keys and services. At the bottom, there is a "VeriSign Secured" logo and a footer with "Política de Privacidad y Uso. Defensoría del Cliente. Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl ©2017 BancoEstado. Todos los derechos reservados."

Whois

Ministerio del Interior y Seguridad Pública

Página 2 de 3

```
soc@kali:~$ whois -h whois.nic.cl terrium.cl
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: terrium.cl
Registrant name: COMERCIAL EPULLEN LIMITADA
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2010-03-02 15:02:43 CLST
Expiration date: 2023-04-01 12:02:04 CLST
Name server: nsl.terrium.cl (108.179.227.230)
Name server: ns2.terrium.cl (108.179.227.229)
```

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- 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