

| | |
|---------------------------------|--|
| Alerta de seguridad cibernética | 8FFR20-00457-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Junio de 2020 |
| Última revisión | 23 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 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:

hxxp://192.119.70[.]33/imagenes/comun2008/login.php

Body SHA-256

d60d4452a7df562ebfa7670b9f0e23f4c89a1bc6079139e7eb84a4d12e0e5187

Certificado Digital

| | | |
|---------------|---|------------|
| Fecha Valido | : | No Incluye |
| Fecha Termino | : | No Incluye |
| Emitido | : | No Incluye |

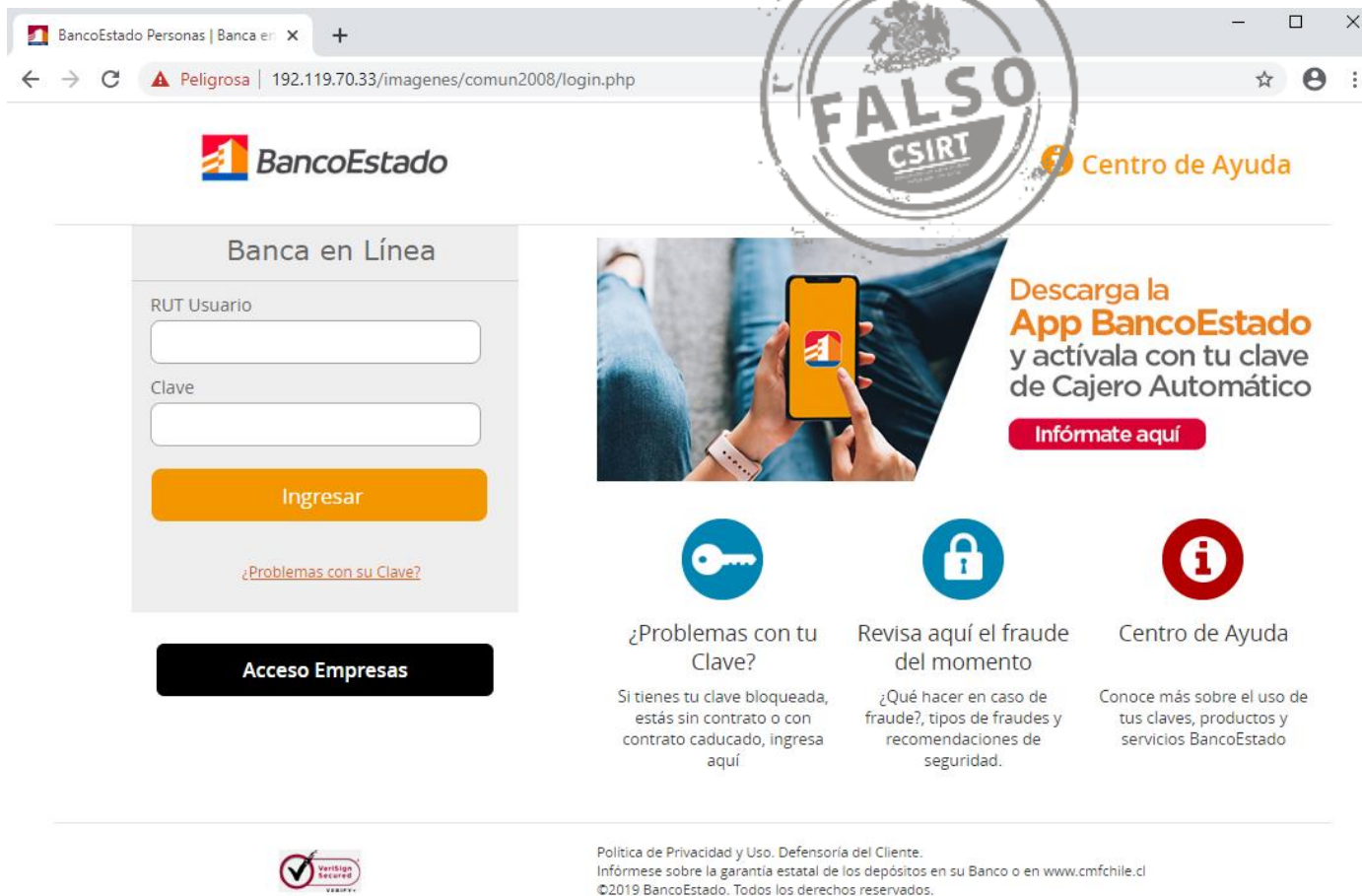
Datos Alojamiento

| | | |
|---------------------------------|---|----------------|
| IP | : | 192.119.70.33 |
| Número de sistema autónomo (AS) | : | 54290 |
| Etiqueta del sistema autónomo | : | Hostwinds LLC |
| País | : | Estados Unidos |
| Registrador | : | ARIN |

Datos del Dominio

| | | |
|-----------------------------|---|------------|
| Nombre de dominio | : | No Incluye |
| Estado del dominio | : | No Incluye |
| Creado | : | No Incluye |
| Expira | : | No Incluye |
| Información del registrador | : | No Incluye |
| ID IANA | : | No Incluye |
| Correo electrónico | : | No Incluye |
| Servidores de nombres | : | No Incluye |

Imagen del sitio



The image shows a screenshot of the BancoEstado website's login page. A large, semi-transparent stamp with the word "FALSO" and the CSIRT logo is overlaid on the page. The browser's address bar shows the URL "192.119.70.33/imagenes/comun2008/login.php" with a "Peligrosa" warning. The login form includes fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "¿Problemas con su Clave?". Below the form is an "Acceso Empresas" button. To the right, there is a promotional banner for the "App BancoEstado" and three service links: "¿Problemas con tu Clave?", "Revisa aquí el fraude del momento", and "Centro de Ayuda". At the bottom, there is a "Verisign Secure" logo and a footer with legal information.

BancoEstado Personas | Banca en línea

Peligrosa | 192.119.70.33/imagenes/comun2008/login.php

BancoEstado Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas

Descarga la **App BancoEstado** y actívala con tu clave de Cajero Automático

Infórmate aquí

¿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.

Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado

Verisign Secure

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.