

Alerta de Seguridad Informática (8FPH-00039-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 25 de Junio de 2019 | Última revisión 25 de Junio de 2019

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 afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC 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 IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco para que vuelvan a activar su cuenta, de lo contrario podría quedar bloqueada. Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

Indicadores de compromisos

Url's:

[http\[://www.tennis-russia\[.\]ru/en/public/personas_bancoestado](http://www.tennis-russia[.]ru/en/public/personas_bancoestado)

[https\[://metroo\[.\]jir/id/home/imagenes/comun2008/banca-en-linea-personas.html](https[://metroo[.]jir/id/home/imagenes/comun2008/banca-en-linea-personas.html)

Smtip Host

seleccion.com [190.114.254.208]

Sender

apache@seleccion[.]com

From (Falso):

BancoEstado <bancoestado@plusconsulting[.]cl>

Subject:

✓ Alerta Cuenta Inhabilitada - (Activar Urgente)

Imagen Phishing correo

ARCHIVO MENSAJE



Alerta Cuenta Inhabilitada - (Activar Urgente) - Mensaje (HTML)

martes 25-06-2019 9:49

BancoEstado <bancoestado@plusconsulting.cl>

✓ Alerta Cuenta Inhabilitada - (Activar Urgente)

Para [Redacted]


 

Estimado(a) [Redacted]

Acabas de realizar una Actualizacion de datos.

Su cuenta muestra segun nuestro sistema un mensaje de **Error: BCE001547-56**, mismo que se define como **CUENTA SUSPENDIDA**, que se ha generado por que usted no ha realizado el proceso de Verificacion de Identidad

Es necesario que ingrese a nuestra web para poder verificar su informacion en nuestra base de datos o de lo contrario su servicio de banca por internet quedara bloqueada y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.

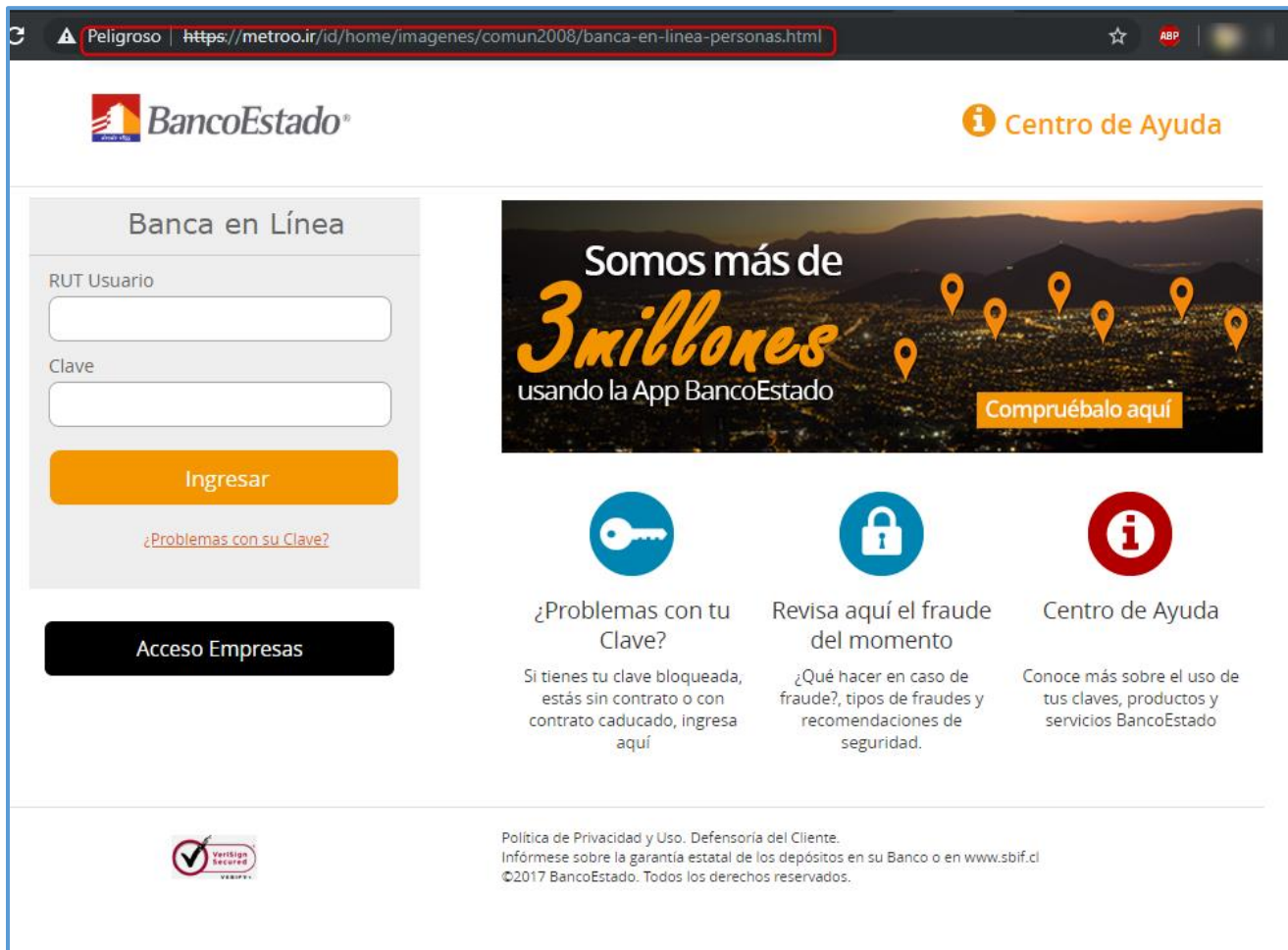
¿Olvidaste tu Clave? 

Ingresando a [Banco Estado - Activacion](#) Usted podra restablecer el acceso a sus cuentas

[\[\] \[Activar Cuenta\]](#)

ⓧ No se pudo mostrar la imagen vinculada. Puede que se haya movido, cambiado de nombre o eliminado el archivo. Compruebe que el vínculo señala al archivo y ubicaciones correctos.

Imagen Sitio Phishing



The screenshot shows a phishing website for BancoEstado. The browser's address bar displays a URL: `https://metroo.ir/id/home/imagenes/comun2008/banca-en-linea-personas.html`, which is highlighted as 'Peligroso' (Dangerous). The website header features the BancoEstado logo and a 'Centro de Ayuda' (Help Center) link. 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 login form is a button for 'Acceso Empresas'. On the right, there is a promotional banner for the BancoEstado app, stating 'Somos más de 3 millones usando la App BancoEstado' and 'Compruébalo aquí'. Below the banner are three columns of links: '¿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). The footer contains a 'Verificación Resguardos' logo and text regarding privacy policy and state deposit guarantees.

BancoEstado Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas

Somos más de **3 millones** usando la App BancoEstado

Compruébalo aquí

¿Problemas con tu Clave?

Revisa aquí el fraude del momento

Centro de Ayuda

Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí

¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.

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


Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbf.cl
©2017 BancoEstado. Todos los derechos reservados.

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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

Contactos

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

 + (562) 24863850

 @CSIRTGOB

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