
Alerta de Seguridad Informática (8FPH-00048-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 24 de Julio de 2019 | Última revisión 24 de Julio 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 de Estado. El correo informa a las víctimas que se realizó un mantenimiento en los servicios del banco y producto de ello, se encontró un error en la cuenta del usuario. Lo anterior obligó al bloqueo de la cuenta, y la única forma de activarla nuevamente es seleccionando el enlace indicado en el correo. De este modo, el atacante intenta convencer al usuario para ingresar al enlace y entregar sus credenciales en un sitio semejante al del banco.

“Estos casos de phishing 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 phishing, 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”

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- [http://theswaggirl\[.\]com/view/Activacion\[.\]php](http://theswaggirl[.]com/view/Activacion[.]php)
- [http://kimochy\[.\]jp/dev/www\[.\]bancoestado\[.\]cl/](http://kimochy[.]jp/dev/www[.]bancoestado[.]cl/)

Smtip Host

- hwsrv-549718[.]hostwinddns[.]com [142.11.214.236]


From:


- apache@hwsrv-549718[.]hostwinddns[.]com

Subject:


- Fwd:Cuenta Bloqueada.

Imagen Phishing Correo

 BancoEstado <noreply@bancoestado.cl>
Fwd:Cuenta Bloqueada.



Estimado(a): msalinas@interior.gov.cl




Banco de Estado, le comunica que se realizo un mantenimiento en nuestros Servicios(Caja Vecina,ServiEstado).Encontramos error en su cuenta.

Debido a este suceso y en cumplimiento con la nueva normativa vigente de seguridad nos vemos en la obligacion de **Bloquear su Cuenta.**

► Su cuenta se activara solo por este E-mail ingresa a:

https://www.bancoestado.cl/Seguridad/Activacion_de_cuenta

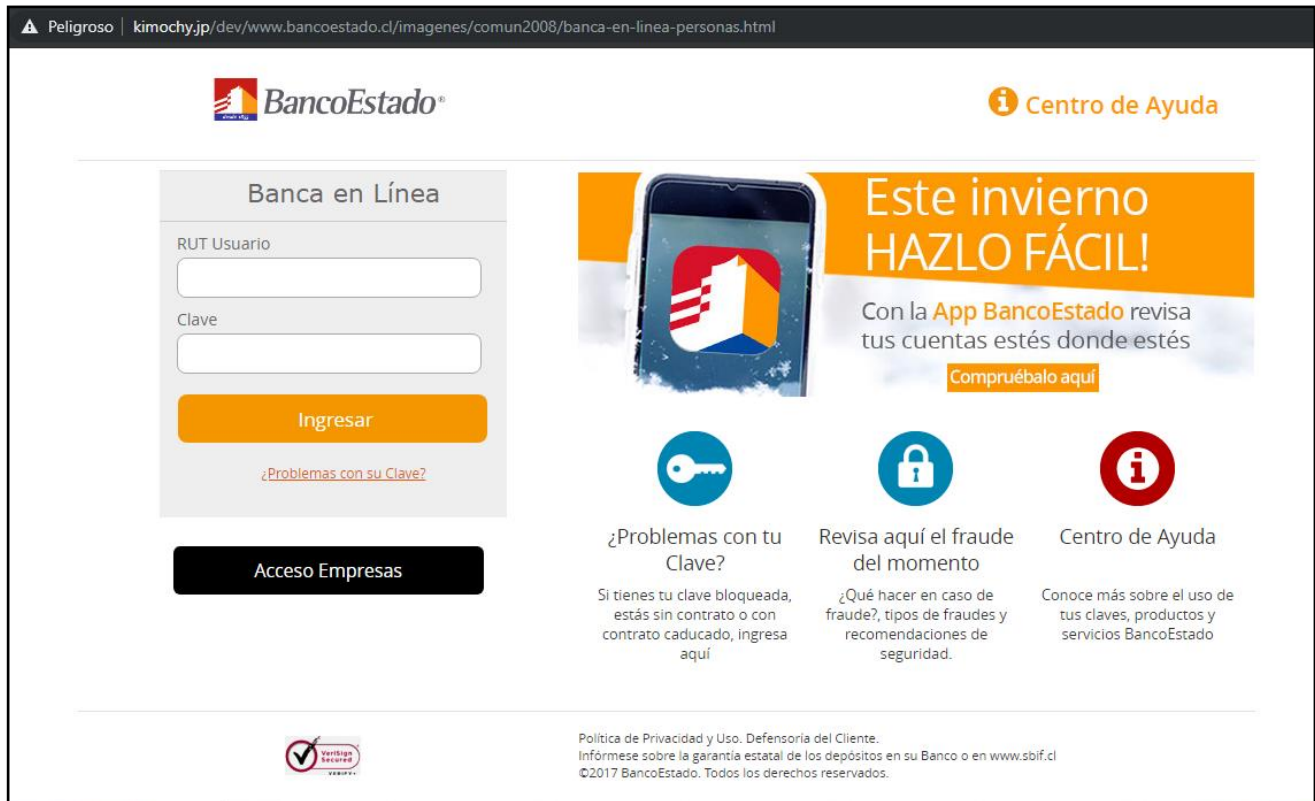


www.bancoestado.cl



Te invitamos a revisar las distintas opciones de **Ahorro e Inversion** que tenemos para ti, desde tu **Banca en Línea.**

600 400 7000 • bancoestado.cl

Imagen Sitio Web



▲ Peligroso | kimochy.jp/dev/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html

 **BancoEstado**  Centro de Ayuda

Banca en Línea


RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)


Acceso Empresas





Este invierno HAZLO FÁCIL!


Con la **App BancoEstado** revisa tus cuentas estés donde estés

Compruébalo 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


 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.

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y 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
- Visualizar los sitios web que se ingresen que sean los oficiales

Contactos

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

 + (562) 24863850

 @CSIRTGOB

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