Alerta de Seguridad Informática (8FPH-00038-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 21 de Junio de 2019 | Última revisión 21 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 registrar su cuenta, de lo contraria 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[:]//csaindia[.]org/test/beneficios/
http[:]//christinaisrael[.]ru/img/router/imagenes/comun2008/banca-en-linea-personas.html

Smtp Host

hwsrv-520556.hostwindsdns.com [142.11.246.200]
hwsrv-520558.hostwindsdns.com [142.11.246.201]

Sender

apache@hwsrv-520556.hostwindsdns[.]com
apache@hwsrv-520558.hostwindsdns[.]com

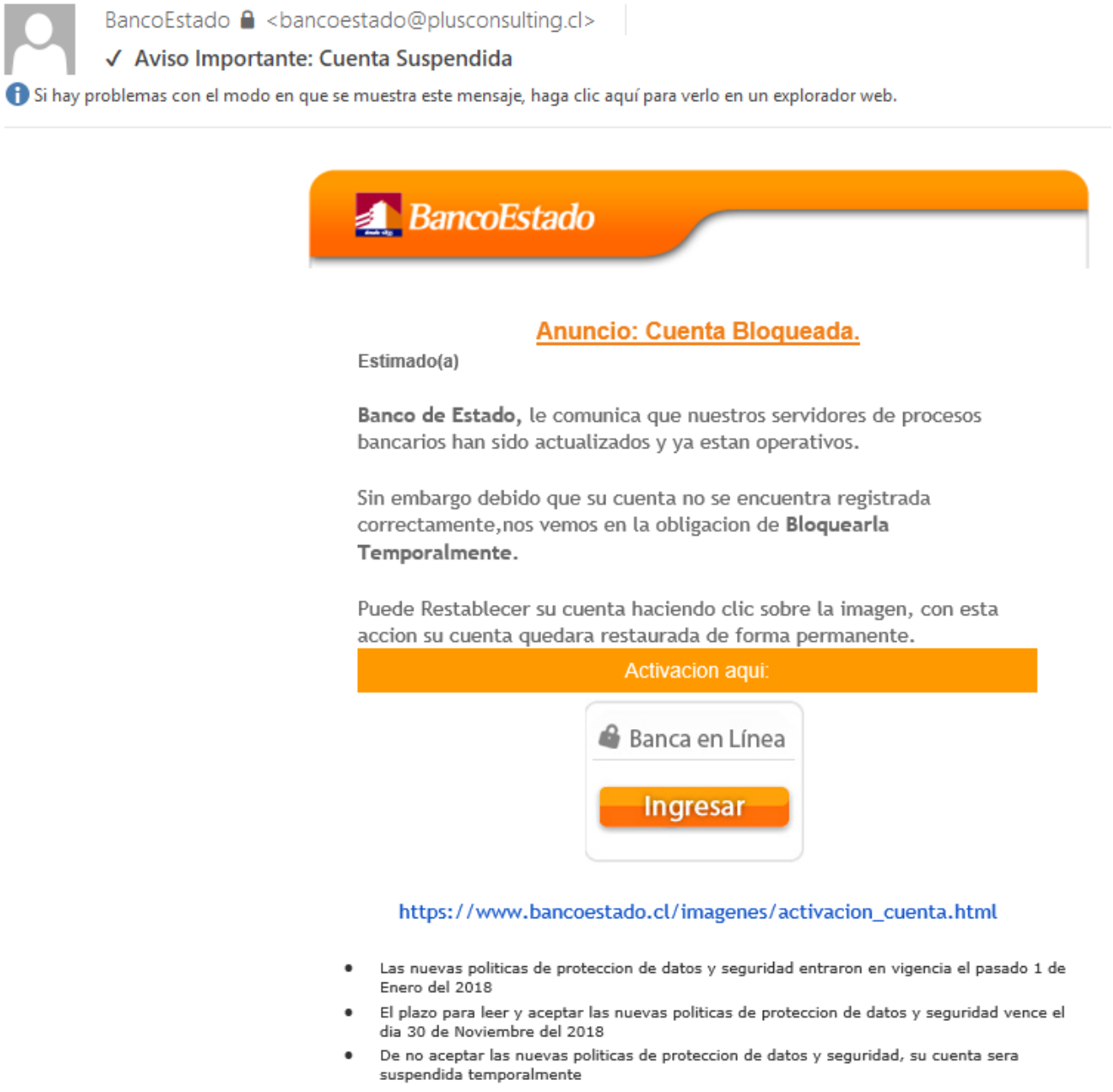
From (Falso):

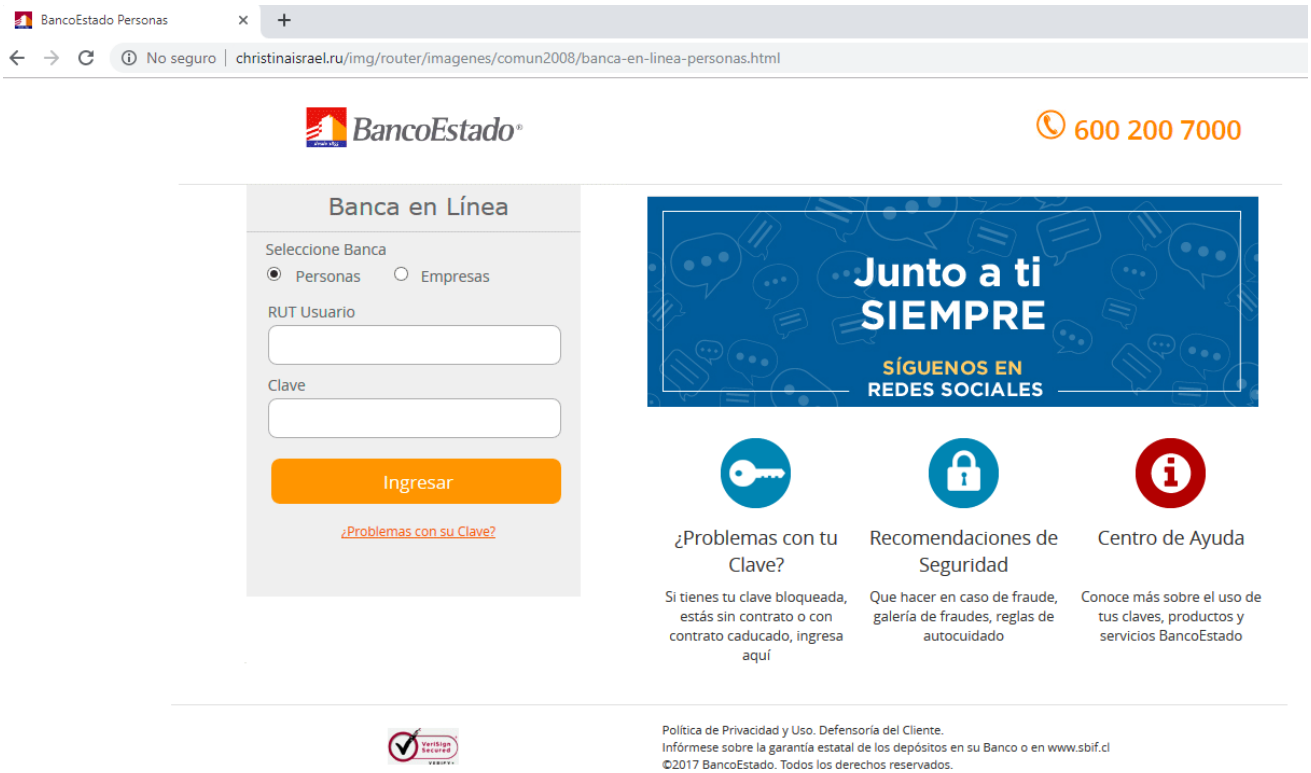
BancoEstado 🔒 <bancoestado@plusconsulting[.]cl>

Subject:

✓ Aviso Importante: Cuenta Suspendida
✓ Fw: Cuenta Suspendida

Imagen


BancoEstado <bancoestado@plusconsulting.cl>
✓ Aviso Importante: Cuenta Suspendida
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.
BancoEstado
Anuncio: Cuenta Bloqueada.
Estimado(a)
Banco de Estado, le comunica que nuestros servidores de procesos bancarios han sido actualizados y ya estan operativos.
Sin embargo debido que su cuenta no se encuentra registrada correctamente,nos vemos en la obligacion de Bloquearla Temporalmente.
Puede Restablecer su cuenta haciendo clic sobre la imagen, con esta accion su cuenta quedara restaurada de forma permanente.
Activacion aqui:
Banca en Línea
Ingresar
https://www.bancoestado.cl/imagenes/activacion_cuenta.html
Las nuevas politicas de proteccion de datos y seguridad entraron en vigencia el pasado 1 de Enero del 2018
El plazo para leer y aceptar las nuevas politicas de proteccion de datos y seguridad vence el dia 30 de Noviembre del 2018
De no aceptar las nuevas politicas de proteccion de datos y seguridad, su cuenta sera suspendida temporalmente


BancoEstado Personas
No seguro | christinaisrael.ru/img/router/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
600 200 7000
Banca en Línea
Seleccione Banca
Personas
Empresas
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Junto a ti SIEMPRE
SÍGUENOS EN REDES SOCIALES
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Recomendaciones de Seguridad
Que hacer en caso de fraude, galería de fraudes, reglas de autocuidado
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, 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