
Alerta de Seguridad Informática (8FPH-00026-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 06 de Junio de 2019 | Última revisión 06 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 afectada 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 para que verifiquen su cuenta ya que, producto de un proceso de actualización de “servidores”, se habría detectado que la cuenta del usuario no estaba registrada. Bajo esa premisa, los delincuentes intentan convencer a sus víctimas para que accedan a los enlaces maliciosos ubicado en el sitio y entregar de esa forma las credenciales de acceso del banco.

Indicadores de compromisos

Url's:

<http://asavage.co.uk/manager/Simuladores/>

<http://elbrus-voda.ru/fast/Simuladores/>

http://gomiles.vn/manager/imagenes/comun2008/nuevo_paglg_pers2.html

http://gomiles.vn/slider/imagenes/_personas/home/default.asp

Smtip Host

rikirikon[.]net [45.7.231.155]

hwsrv-510633.hostwinddns[.]com [104.168.211.27]

From:

apache@rikirikon.net

apache@hwsrv-510633.hostwinddns.com

Subject:

- ✓ Fw: Notificacion- Cuenta Bloqueada
- ✓ Fw: Cuenta Temporalmente Bloqueada

Imagen



NOTIFICACION: Cuenta Bloqueada.

Estimado(a):

BancoEstado, 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:



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 2019
- El plazo para leer y aceptar las nuevas politicas de proteccion de datos y seguridad vence el dia 30 de Noviembre del 2019
- De no aceptar las nuevas politicas de proteccion de datos y seguridad, su cuenta sera Bloqueada temporalmente



📞 600 200 7000

Banca en Línea

Seleccione Banca

Personas Empresas

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)



¿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>