

Alerta de Seguridad Informática (8FPH-00023-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 24 de Mayo de 2019 | Última revisión 24 de Mayo 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 del Banco para que vuelvan a registrar 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:

[https://keytolifeblog\[.\]com/wp-includes/Activacion.php](https://keytolifeblog[.]com/wp-includes/Activacion.php)

[http://evmade\[.\]com/docs/www\[.\]bancoestado\[.\]cl/imagenes/comun2008/banca-en-linea-personas.html](http://evmade[.]com/docs/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas.html)

Smtip Host

apache@hwsrv-496855.hostwinddns[.]com

apache@hwsrv-496824.hostwinddns[.]com

apache@hwsrv-496823.hostwinddns[.]com

apache@hwsrv-493714.hostwinddns[.]com

From:

apache@localhost

Subject:

✓ Aviso Importante: Cuenta Bloqueada
Fw:Cuenta Bloqueada.

Imagen



BancoEstado | CON TODOS PARA TODOS
CORREDORES DE SEGUROS

Vive
con tranquilidad.

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. solo podra hacerlo por medio de este e-mail.

Para activar su cuenta ingrese Aqui. 

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

www.bancoestado.cl





CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

⚠ Sitio web no seguro | evmade.com/docs/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html



i Centro de Ayuda

Banca en Línea

RUT Usuario

Clave

Ingresar

[¿Problemas con su Clave?](#)

Acceso Empresas

Ya somos más de 3.000.000 usando la App BancoEstado

¡Únete tú también y simplifica tu vida!



¿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.
Informe 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>