Alerta de Seguridad Informática (8FPH-00022-001)

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 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 para que verifiquen su tarjeta de coordenadas registrada en la web debido a la incertidumbre del Banco ante una posible intervención de terceros en la cuenta del usuario. Bajo esa premisa, los delincuentes intentan convencer a sus víctimas para que accedan a los enlaces maliciosos ubicado en el sitio.

Indicadores de compromisos

Url's:

http[:]//elbrus-voda[.]ru/fast/Simuladores/

http[:]//apnarigs[.]com/action/onp/imagenes/comun2008/nuevo_paglg_pers2[.]html

Smtp Host

apache@hwsrv-501276[.]hostwindsdns[.]com
apache@hwsrv-494522[.]hostwindsdns[.]com
apache@hwsrv-494154[.]hostwindsdns[.]com

From:

apache@localhost

Subject:

✓ Fw: Actividad Inusual (Cuenta Deshabilitada)

Imagen

BancoEstado

Numero de folio: 57E3CLB8E

Estimado cliente:

Banco Estado necesita verificar su Tarjeta De Coordenadas registrado en nuestra banca por Internet, esta operacion requiere ser atendida para poder ingresar a sus cuentas afiliadas a BancoEstado en linea.

Tenemos la incertidumbre de que su cuenta haya podido ser tomado por un tercero. Debido a que la proteccion y seguridad de su cuenta corre por nuestra parte, hemos limitado el acceso en linea de modo temporal, esta medida es tomada con eventualidad en caso de proteccion y es levantado un Reporte del Mismo. ID243-048.017.

El numero de su comprobante de Operacion es: AD-001-3072.

Para actualizar tus datos de manera segura haz click en el boton Ingresar.

Ingresar

VeriSign Secured VERIFICAR

PagoRUT

Tarifado Productos y Tasas de Interes
Política de Privacidad - Guía del Cliente Bancario (SBIF)
Codigo de Conducta y Buenas Practicas de Bancos e Instituciones Financieras
Informese sobre la garantía estatal de los depositos en su Banco o en www.sbif.cl Â© 2017
BancoEstado.cl. Todos los derechos reservados

DEFENSORÍA DEL CLIENTE

**Recuerde que el hacer caso omiso de Ã©ste mensaje puede poner en riesgo la seguridad de tu cuenta.*


apnarigs.com/action/onp/imagenes/comun2008/nuevo_paglg_pers2.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

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