

Alerta de seguridad cibernética	8FFR20-00823-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Noviembre de 2020
Última revisión	07 de Noviembre de 2020

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 loC 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 loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude 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 fraude, 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de una pagina fraudulenta asociada a un dominio .com que intenta suplantar al sitio de Banco Estado, el que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

Indicadores de compromiso

URL sitio falso

http[:]//zax-associates[.]com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html

Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

Certificado Digital

Fecha Válido	No disponible
Fecha Término	No disponible
Emitido	No disponible

Datos Alojamiento

IP	91[.]220[.]196[.]145
Número de Sistema Autónomo (AS)	50304
Etiqueta del Sistema Autónomo	Blix Solutions AS
País	NO
Registrador	RIPE NCC

Datos del Dominio

Nombre de Dominio	ZaX-Associates[.]com
Creado	28/11/2010
Expira	28/11/2020
Información del Registrador	GoDaddy.com, LLC
ID IANA	146
Correo Electrónico	abuse@godaddy.com
Name Server	NS1.RUNBOX.NET NS2.RUNBOX.NET

Imagen del sitio

zax-associates.com/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html



The screenshot shows the BancoEstado online banking interface. At the top left is the BancoEstado logo. To the right is a 'Centro de Ayuda' (Help Center) link. The main content area is titled 'Banca en Línea' and contains a login form with fields for 'RUT Usuario' and 'Clave', an 'Ingresar' button, and a link for '¿Problemas con su Clave?'. Below the login form is an 'Acceso Empresas' button. To the right of the login form is a promotional banner for the 'App BancoEstado' with a download button. Below the banner are three circular icons: a key, a padlock, and an information icon. Each icon has a corresponding text block: '¿Problemas con tu Clave?' (with a CSIRT stamp), 'Revisa aquí el fraude del momento', and 'Centro de Ayuda'. At the bottom left is a 'Verificación Segura' logo, and at the bottom right is a footer with privacy policy information.



Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- 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 sean los oficiales.