

Alerta de seguridad cibernética	8FFR20-00465-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Junio de 2020
Última revisión	29 de Junio 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 un portal fraudulento asociado a un dominio que suplanta el sitio web oficial de **Banco Estado**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

Indicadores de compromiso

Urls sitio falso:

hxxps://gharaviri.ir/Pension/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html

Body SHA-256

338a24e2206d3b76f8a9c7364991fbada0908b7432c66a294645e7cc5f937d5d

Certificado Digital

Fecha Valido	:	No Aplica
Fecha Termino	:	No Aplica
Emitido	:	No Aplica

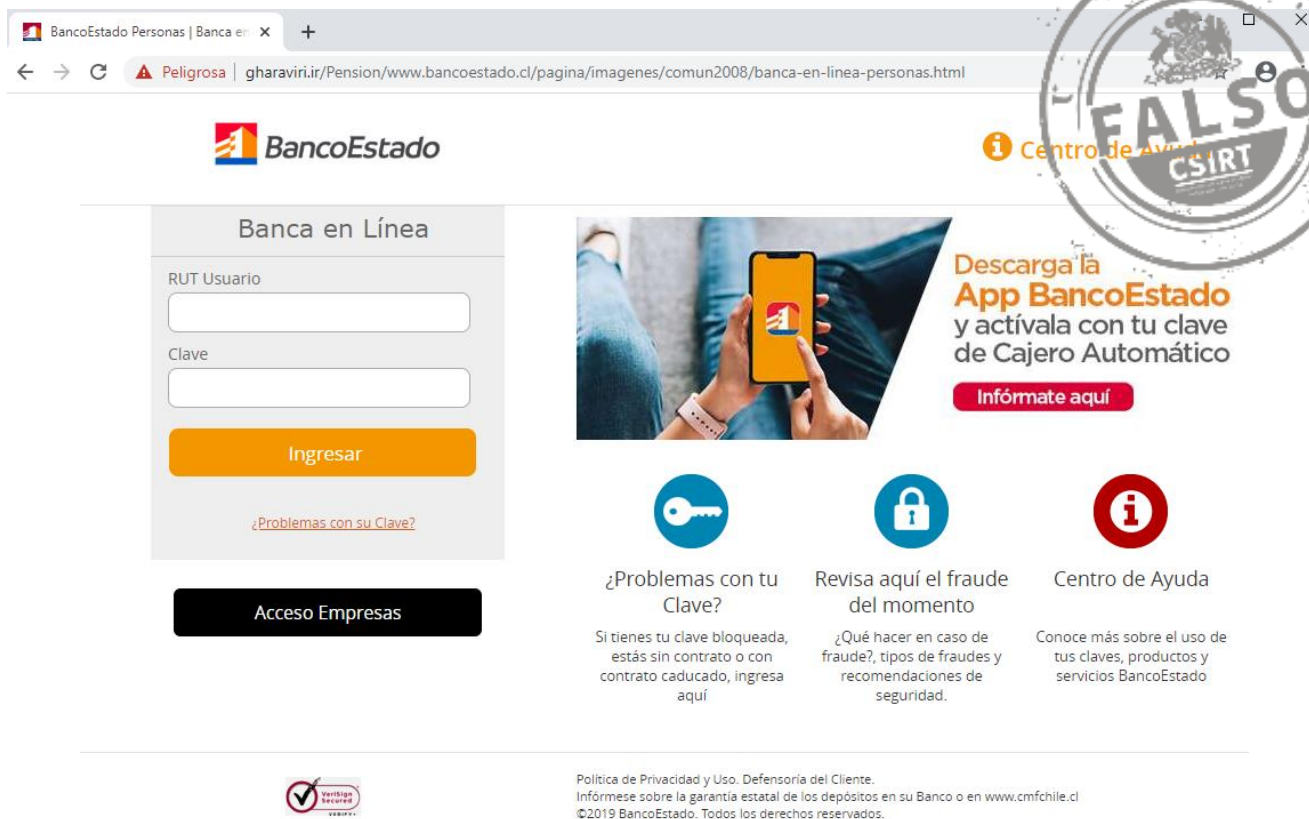
Datos Alojamiento

IP	:	185.105.185.20
Número de sistema autónomo (AS)	:	25264
Etiqueta del sistema autónomo	:	RIPER
País	:	IRAN
Registrador	:	RIPE NCC

Datos del Dominio

Nombre de dominio	:	gharaviri.ir
Estado del dominio	:	clientTransferProhibited addPeriod
Creado	:	20-01-2012
Expira	:	10-01-2021
Información del registrador	:	Fanavarie Etelaate Towseye Saman
ID IANA	:	to52-irnic
Correo electrónico	:	sales@mihannic.com
Servidores de nombres	:	ns3.mihanmizban.net, ns4.mihanmizban.ne

Imagen del sitio



The screenshot shows a web browser window with the URL gcharaviri.ir/Pension/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html. The page features the BancoEstado logo and a login form titled "Banca en Línea" with fields for "RUT Usuario" and "Clave", an "Ingresar" button, and a link for "¿Problemas con su Clave?". Below the form is an "Acceso Empresas" button. To the right, there is a promotional banner for the "App BancoEstado" with a "Descarga la App BancoEstado y actívala con tu clave de Cajero Automático" message and an "Infórmate aquí" button. Three circular icons represent: "¿Problemas con tu Clave?", "Revisa aquí el fraude del momento", and "Centro de Ayuda". A large, semi-transparent "FALSO" watermark is overlaid on the right side of the page. At the bottom, there is a "Verificado" seal and a footer with the text: "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.