

Alerta de seguridad cibernética	8FFR20-00761-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de Septiembre de 2020
Última revisión	30 de Septiembre 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 afectada 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 aludida.

Indicadores de compromiso

Urls sitio falso:

bancedelestado[.]ddns[.]net

Body SHA-256

e2af7c63ec10394c76345311f7d8e667e3ebbc081653e9ad58bb7412069579

Certificado Digital

Fecha Valido : 2020-09-29 00:03:08
Fecha Termino : 2020-12-28 00:03:08
Emitido : Let's Encrypt Authority X3

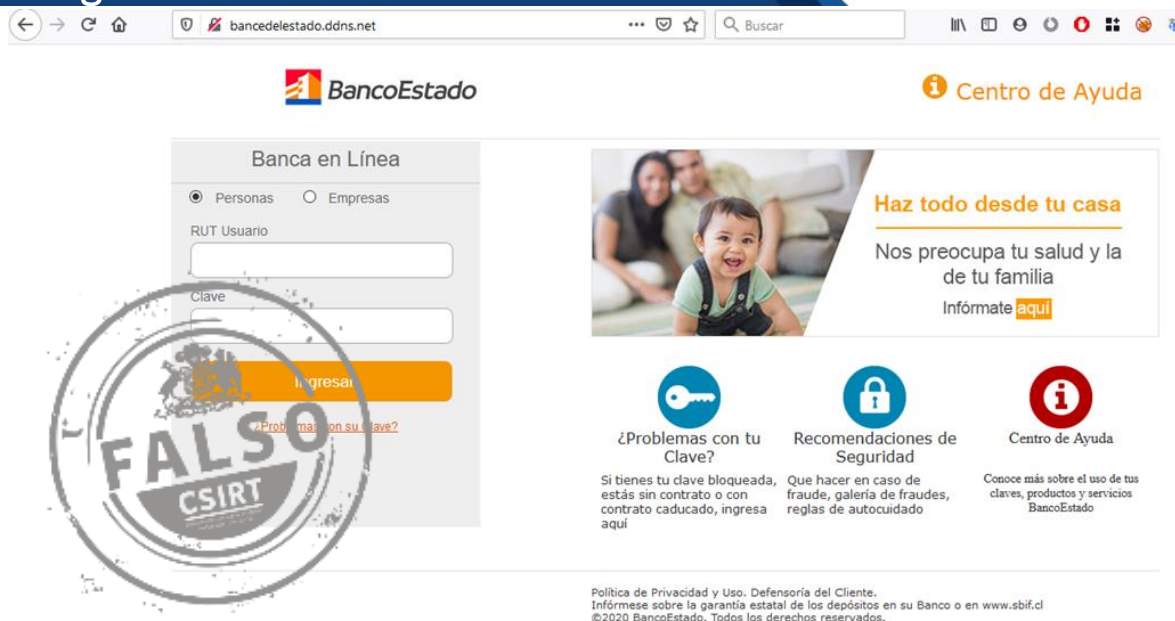
Datos Alojamiento

IP : 217[.]195[.]153[.]128
Número de sistema autónomo (AS) : 395092
Etiqueta del sistema autónomo : Shock Hosting LLC
País : Holanda
Registrador : ripe

Datos del Dominio

Nombre de dominio : ddns[.]net
Estado del dominio : Activo
Creado : 2001-06-28T16:04:59Z
Expira : 2022-06-28T16:04:59Z
Información del registrador : TLDS LLC. d/b/a SRSPlus
ID IANA : 320
Correo electrónico : abuse@web[.]com
Servidores de nombres : nf2[.]no-ip[.]com
nf1[.]no-ip[.]com
nf4[.]no-ip[.]com
nf3[.]no-ip[.]com

Imagen del sitio



The screenshot shows the BancoEstado website interface. At the top left is the BancoEstado logo. To the right is a 'Centro de Ayuda' link. The main content area is divided into two sections. On the left is the 'Banca en Línea' login form, which includes radio buttons for 'Personas' and 'Empresas', input fields for 'RUT Usuario' and 'Clave', and an 'Ingresar' button. A large, semi-transparent watermark with the text 'FALSO CSIRT' is overlaid on the login form. On the right is a promotional banner with the headline 'Haz todo desde tu casa' and the text 'Nos preocupa tu salud y la de tu familia. Infórmate aquí'. Below the banner are three columns of links: '¿Problemas con tu Clave?' (with a key icon), 'Recomendaciones de Seguridad' (with a padlock icon), and 'Centro de Ayuda' (with an information icon). At the bottom of the page, there is 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.sbif.cl ©2020 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.