

Alerta de seguridad cibernética	8FFR20-00852-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de Diciembre de 2020
Última revisión	15 de Diciembre 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 página fraudulenta asociada al dominio .online que intenta suplantar a empresa financiera del Banco Santander, 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

[https://service-santder-cl\[.\]info/1608061556/index.asp](https://service-santder-cl[.]info/1608061556/index.asp)

### Body SHA-256

6d363b8903202fc5aea7d88a249ee79146eb61def26229eaf95ce85209cc7a8c

### Certificado Digital

Fecha Válido	15-12-2020
Fecha Término	15-03-2021
Emitido	Let's Encrypt

### Datos Alojamiento

IP	[167.71.233.97]
Número de Sistema Autónomo (AS)	14061
Etiqueta del Sistema Autónomo	DigitalOcean, LLC
País	IN
Registrador	APNIC

### Datos del Dominio

Nombre de Dominio	service-santder-cl[.]info
Creado	14-12-2020
Expira	14-12-2021
Información del Registrador	Namecheap Inc
ID IANA	1068
Correo Electrónico	abuse@namecheap.com
Name Server	dns1.namecheaphosting.com dns2.namecheaphosting.com

## Imagen del sitio



## 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.