

Alerta de seguridad cibernética	8FFR20-00756-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de Septiembre de 2020
Última revisión	29 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 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 Santander**, 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:

www-santander[.]cl[.]ariesinsumos[.]cl/pagina/login[.]asp

### Body SHA-256

5ade6c04e94d88e4a6e22bf473874ee49e8c9a8b14b9de9239b594a3dd798488

### Certificado Digital

Fecha Valido : domingo, 27 de septiembre de 2020  
21:00:00  
Fecha Termino : domingo, 27 de diciembre de 2020  
20:59:59  
Emitido : cPanel, Inc..

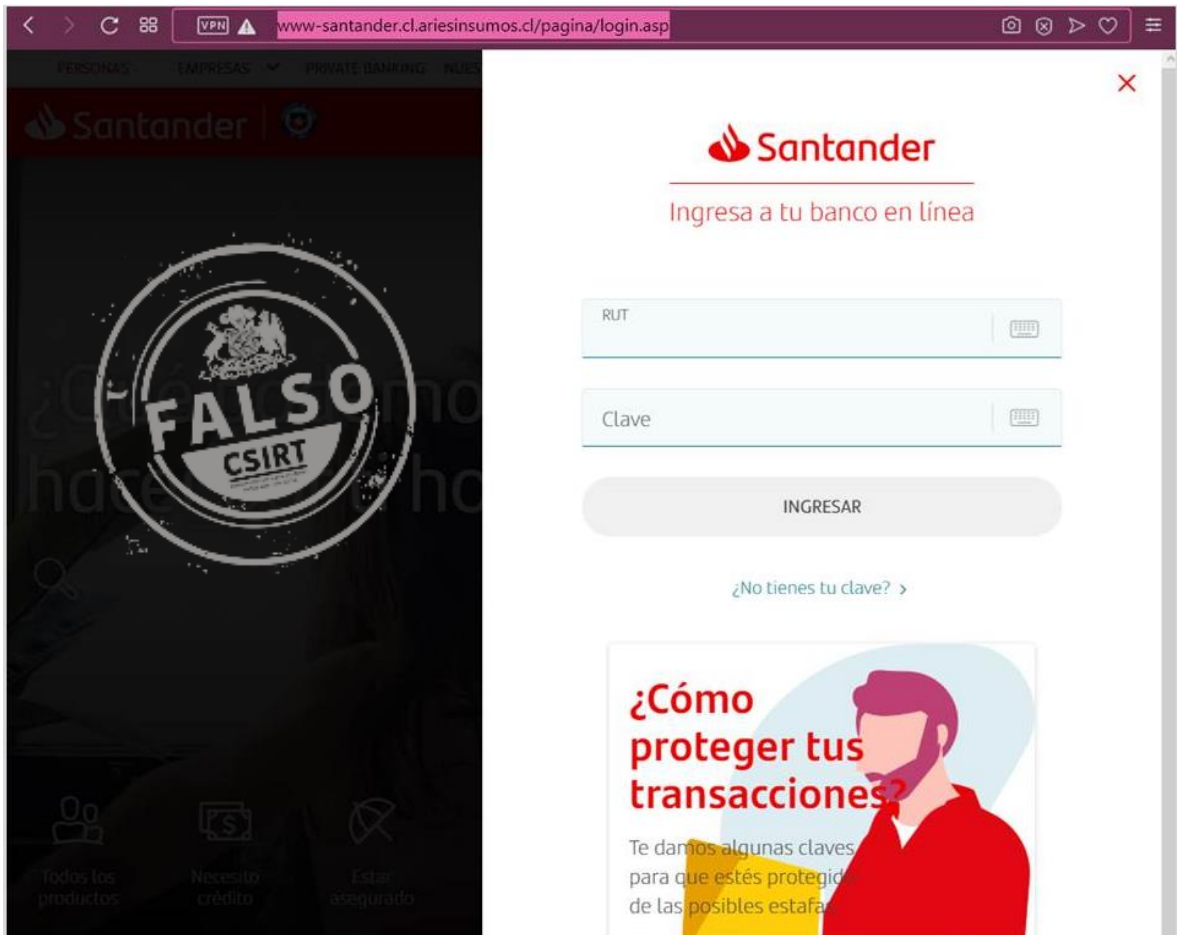
### Datos Alojamiento

IP : 199[.]58[.]186[.]108  
Número de sistema autónomo (AS) : 46562  
Etiqueta del sistema autónomo : Total Server Solutions L.L.C.  
País : Estados Unidos  
Registrador : ARIN

### Datos del Dominio

Nombre de dominio : ariesinsumos[.]cl  
Estado del dominio : Activo  
Creado : 2016-06-24 16:41:41 CLST  
Expira : 2021-06-24 16:41:41 CLST  
Información del registrador : Orlando Enrique Torres Garrido  
ID IANA : No Registrado  
Correo electrónico : No Registrado  
Servidores de nombres : ns4[.]chileserver[.]net  
ns3[.]chileserver[.]net

## 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.