

Alerta de seguridad cibernética	8FFR20-00754-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de Septiembre de 2020
Última revisión	28 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 **Scotiabank**, 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:

scotiabankchle-infos[.]ml

### Body SHA-256

1da65ecf52e483bffd96f5db029e9a6be99498ef2817e5c6ad0f970c7524480

### Certificado Digital

Fecha Valido : domingo, 27 de septiembre de 2020  
20:49:03  
Fecha Termino : sábado, 26 de diciembre de 2020 20:49:03  
Emitido : Let's Encrypt

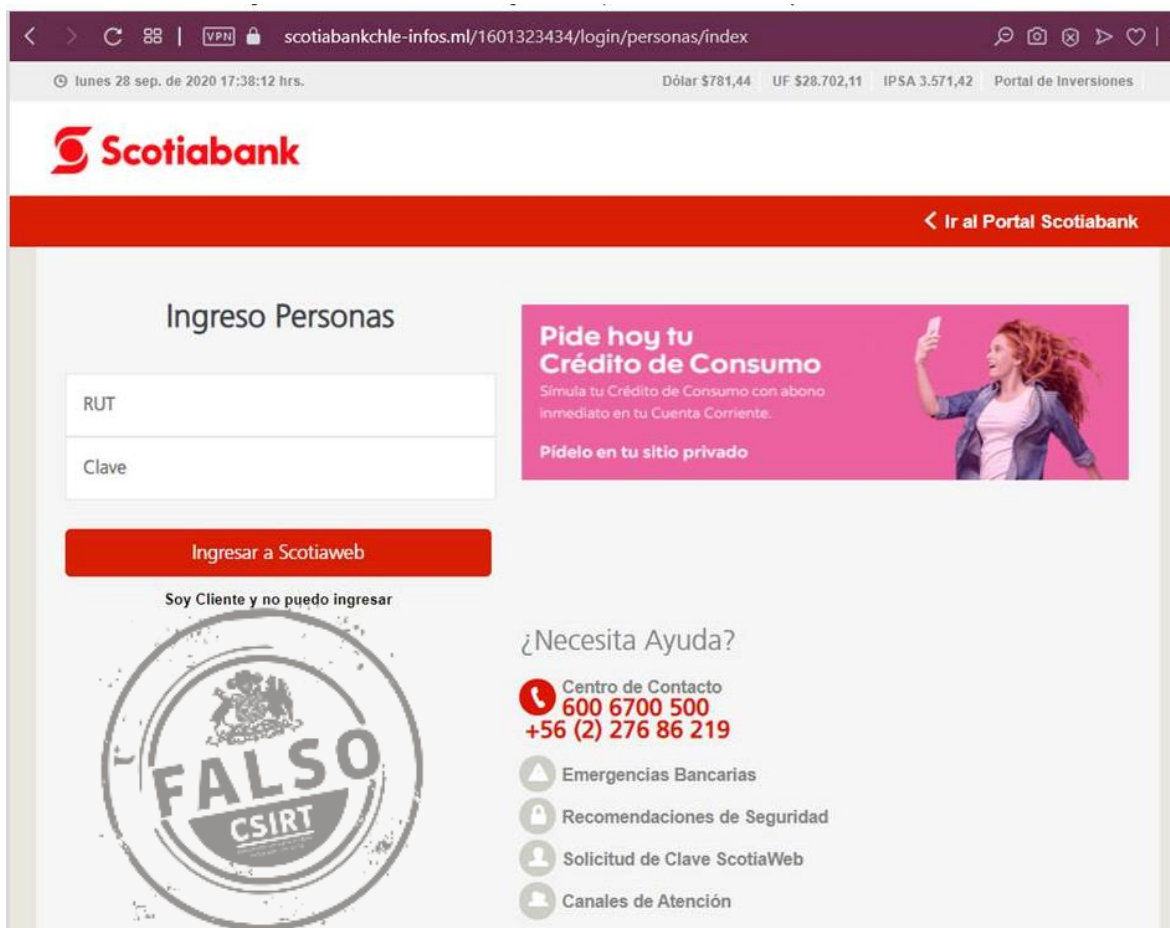
### Datos Alojamiento

IP : 178[.]159[.]36[.]141  
Número de sistema autónomo (AS) : 48666  
Etiqueta del sistema autónomo : MAROSNET Telecommunication Company  
LLC  
País : Rusia  
Registrador : RIPE NCC

### Datos del Dominio

Nombre de dominio : SCOTIABANKCHLE-INFOS[.]ML  
Estado del dominio : Activo  
Creado : No Registrado  
Expira : No Registrado  
Información del registrador : Mali Dili B.V.  
ID IANA : No Registrado  
Correo electrónico : No Registrado  
Servidores de nombres : NS01[.]FREENOM[.]COM  
NS02[.]FREENOM[.]COM  
NS03[.]FREENOM[.]COM  
NS04[.]FREENOM[.]COM

## Imagen del sitio



The screenshot shows the Scotiabank login page for Chile. The browser address bar displays the URL `scotiabankchle-infos.ml/1601323434/login/personas/index`. The page features the Scotiabank logo at the top left and a navigation link "Ir al Portal Scotiabank" at the top right. The main heading is "Ingreso Personas". Below it are two input fields for "RUT" and "Clave", followed by a red "Ingresar a Scotiaweb" button. A message states "Soy Cliente y no puedo ingresar" with a large circular stamp that says "FALSO CSIRT". To the right, there is a promotional banner for "Pide hoy tu Crédito de Consumo" with a woman holding a phone. Below the banner, a section titled "¿Necesita Ayuda?" lists contact options: "Centro de Contacto 600 6700 500 +56 (2) 276 86 219", "Emergencias Bancarias", "Recomendaciones de Seguridad", "Solicitud de Clave ScotiaWeb", and "Canales de Atención".

## 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.