

Alerta de seguridad cibernética	8FFR22-01047-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de enero de 2022
Última revisión	7 de enero de 2022

## 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 IoC 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 IoC 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 del Gobierno de Chile (CSIRT de Gobierno) ha identificado la activación de una página fraudulenta que suplanta al Banco Ripley, la que podría servir para robar credenciales de sus 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 redireccion

<https://bit.ly/3zbRsMK?|=www.bancoripley.cl>  
<http://stz-fmba.ru/wp-includes/certificates/enviar02.php?l=509398429>  
<https://sspmprimaryschool.com/activacion/cuenta-pqdw/>

### URL sitio falso

<https://www-bancoripley-cl.mightytechs.in/1641489095/login>

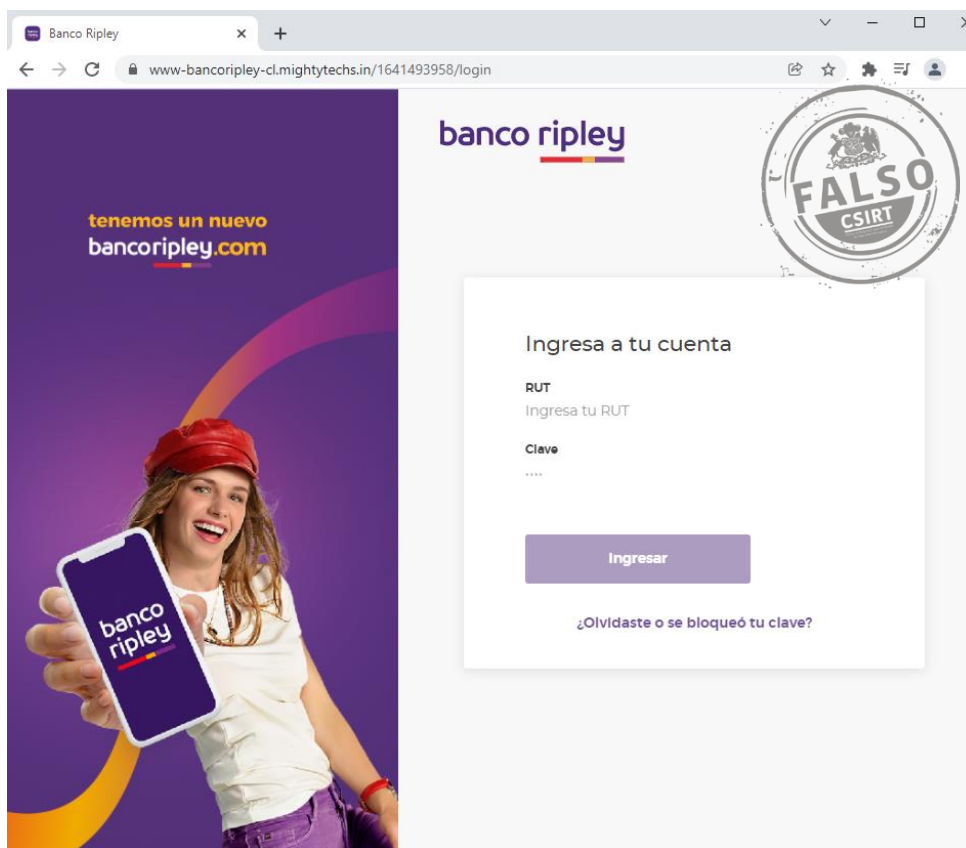
### Certificado Digital

Fecha Válido	05-01-2022
Fecha Término	05-04-2022
Emitido	Let's Encrypt R3

### Datos Alojamiento

IP	[194.233.72.106]
Número de Sistema Autónomo (AS)	141995
Etiqueta del Sistema Autónomo	Contabo Asia Private Limited
País	SG
Registrador	APNIC

## 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 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 toda plataforma de tecnología 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.
- Asegurarse de que los sitios web a los que se ingrese sean los oficiales.