

Alerta de seguridad informática	8FPH21-00456-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de diciembre de 2021
Última revisión	28 de diciembre de 2021

## 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 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 phishing 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 phishing, 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 de Gobierno) advierte sobre una campaña de phishing que está siendo difundida a través de un correo electrónico que se hace pasar como proviene del Banco Ripley.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del email. Para ello, el mensaje del correo indica falsamente que se ha detectado un actividad sospechosa de la última consulta realizada desde la cuenta del destinatario, y que por seguridad su tarjeta ha sido bloqueada temporalmente.

Si hacen clic en el enlace, las personas son dirigidas a un sitio falso, donde se exponen al robo de datos confidenciales.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromiso

**URL redirección:**

hXXps://bit[.]ly/3yQftc9?l=www.bancoripley.cl

**URL sitio falso:**

hXXps://www-bancoripley-cl.tractari-bistrita[.]ro/1640722093/login

**Asunto:**

Fwd:Alerta de Seguridad - TarjetaRipley Bloqueada.

**Correo Electrónico:**

@kalisao.net

**SMTP Host:**

[170.239.84.62]

## Otros antecedentes

### Certificado Digital

Fecha Valido : 27-12-2021  
Fecha Término : 28-03-2022  
Emitido : cPanel, Inc. Certification Authority

### Datos Alojamiento

IP : [185.181.101.3  
Número de sistema autónomo (AS) : 9009  
Etiqueta del sistema autónomo : M247 Ltd  
País : RO  
Registrador : RIPE NCC

### Datos del Dominio

Nombre de dominio : tractari-bistrita[.]ro  
Creado : 01-12-2015  
Expira : NO APLICA  
Información del registrador : ICI - Registrar  
ID IANA : NO APLICA  
Correo electrónico : NO APLICA  
Servidores de nombres : ns1.refreshsite.ro  
ns2.refreshsite.ro

## Imagen del mensaje

Fwd:Alerta de Seguridad - TarjetaRipley Bloqueada.

**B** BancoRipley <mensajeria@mensajeriaripley.cl>  
Lun 27-12-2021 12:30  
Para: Usted



BancoRipley,le informa que se detecto actividad sospechosa en su cuenta, esto es debido a su ultima consulta que realizo por cajero o banca en linea no finalizo de manera correcta.

Por tu Seguridad su cuenta y tarjeta fue bloqueada temporalmente y necesitamos realizar que la verificacion de identidad.Para Verifica su identidad. Haz click [aqui](#)

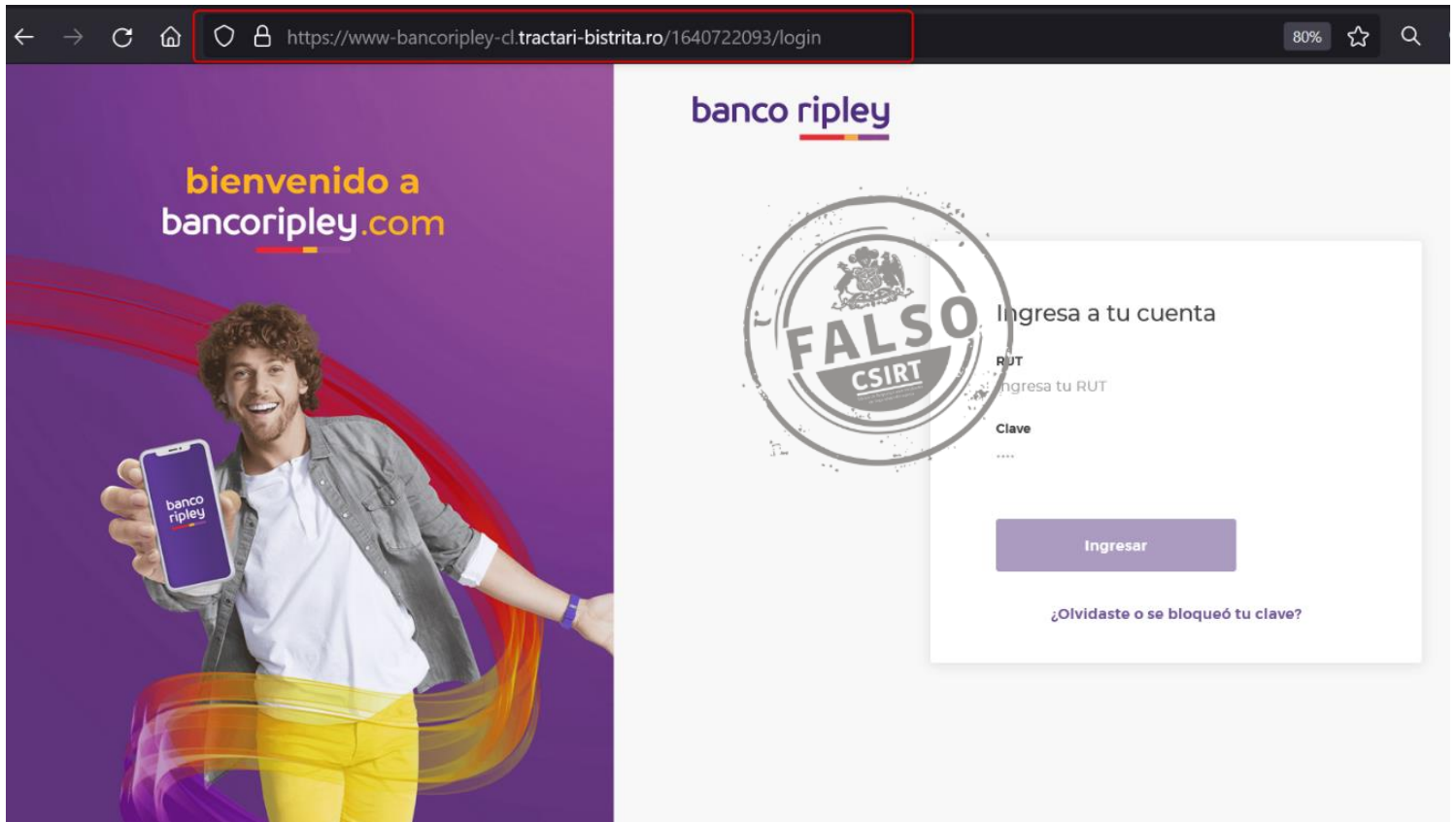
Es necesario que ingrese a nuestra web para poder verificar su informacion en nuestra base de datos o de lo contrario su servicio de banca por internet quedara BLOQUEADA y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.

**ite recomendamos!**

Valida tu Identidad,CONFIRMA TU DATOS y listo!

[Ingresa aqui](#)

## 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.