Alerta de seguridad informática	8FPH22-00464-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2022
Última revisión	14 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 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 se está difundiendo a través de un correo electrónico que supuestamente proviene de Banco Ripley.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del correo.

El mensaje del correo indica falsamente que “se ha detectado actividad sospechosa de la última consulta realizada desde su cuenta y por seguridad la tarjeta ha sido bloqueada temporalmente”. De hacer 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/3tvNQ7g?l=www.bancoripley.cl
hXXps://sspmprimaryschool[.]com/activacion/cuenta-ndln/

URL sitio falso:

hXXps://wwwbancoripley-cl.mightytechs[.]in/1642101336/Login

Asunto:

Fwd:Tu TarjetaRipley Será Bloqueada. ¡Contáctanos!

Correo Electrónico:

@tripitatuex.net

SMTP Host:

[170.239.85.155]

Otros antecedentes

Certificado Digital

Fecha Válido	:	30-12-2021
Fecha Término	:	30-12-2022
Emitido	:	PortSwigger CA

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

Datos del Dominio

Nombre de dominio	:	mightytechs[.]in
Creado	:	06-09-2021
Expira	:	06-09-2022
Información del registrador	:	GoDaddy.com, LLC
ID IANA	:	146
Correo electrónico	:	NO APLICA
Servidores de nombres	:	ns1.highhost.in ns2.highhost.in

Imagen del mensaje

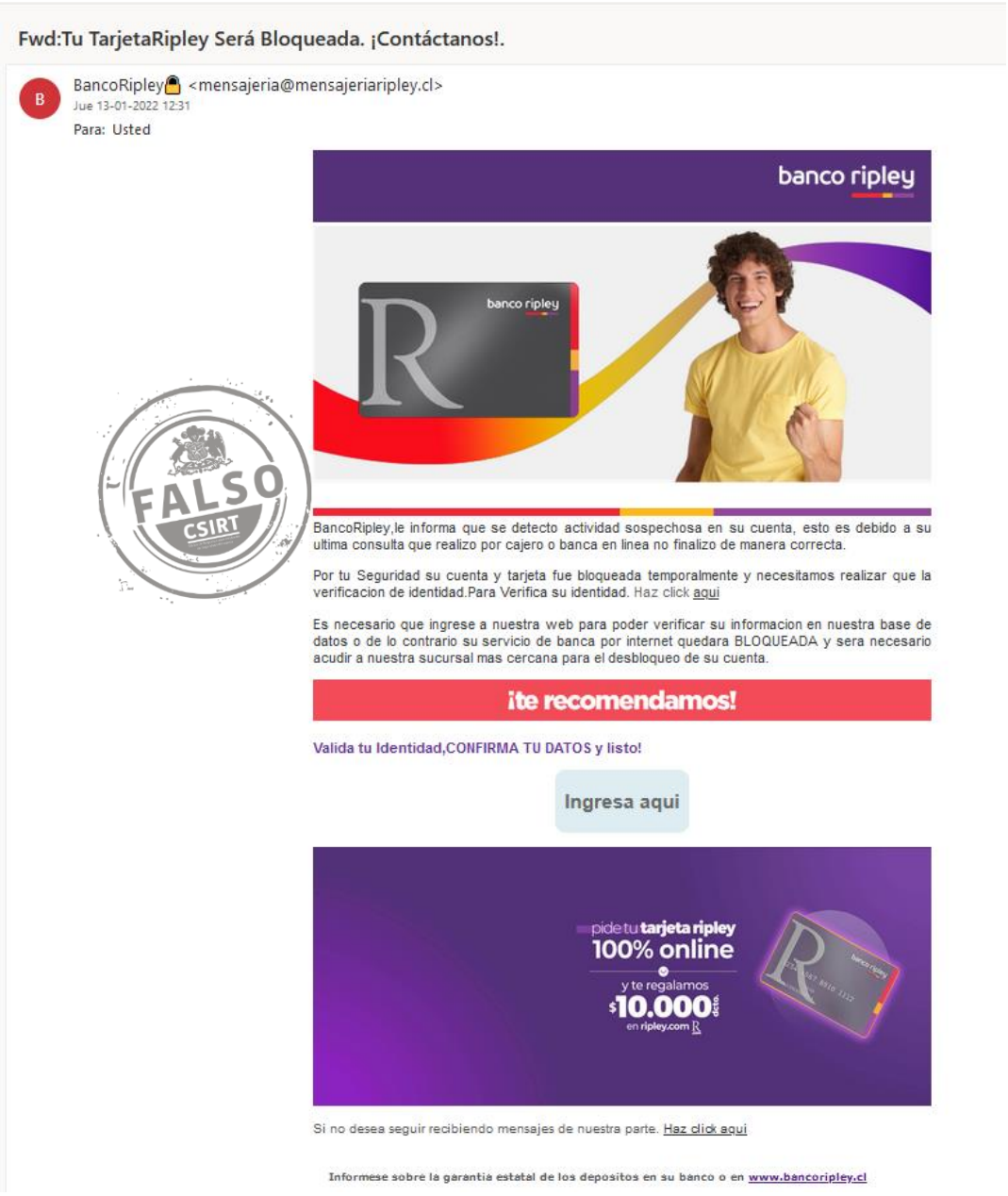
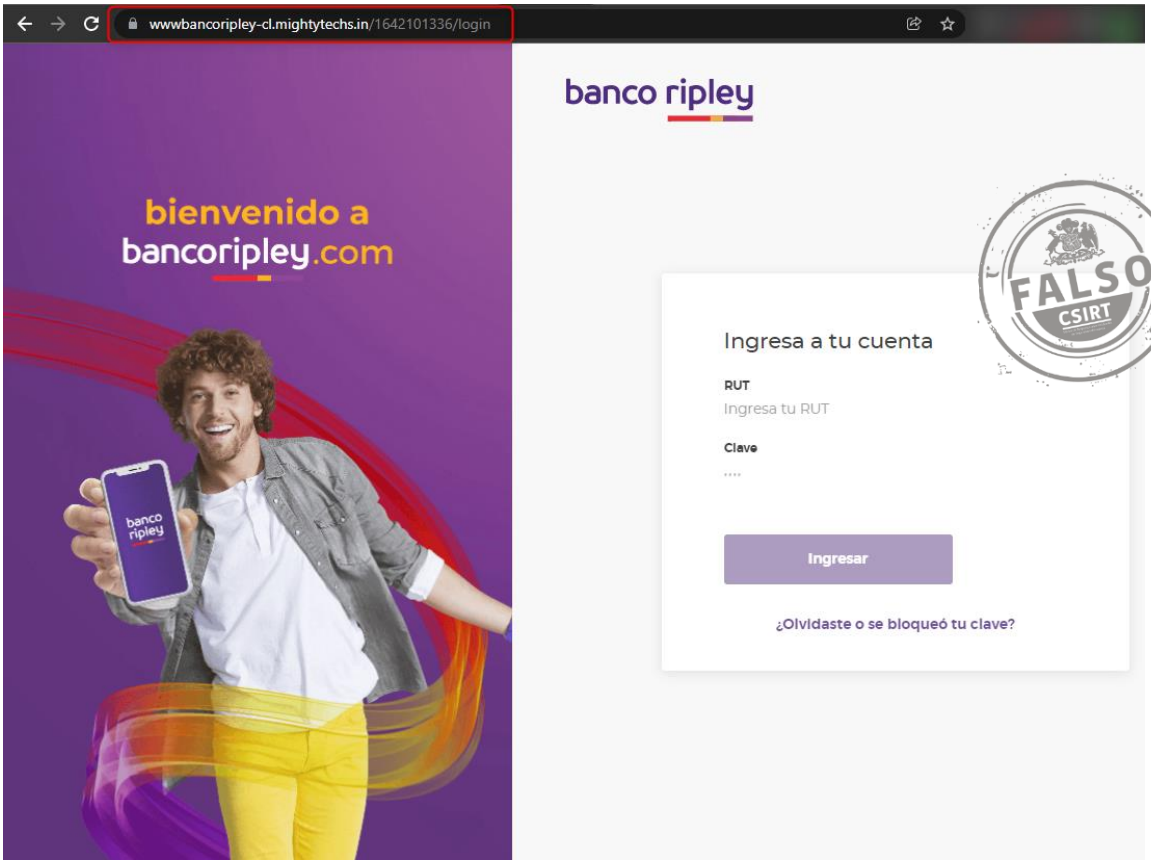


Imagen del sitio



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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.01.14 09:36:26 -03'00'