Alerta de seguridad informática	8FPH21-00435-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de septiembre de 2021
Última revisión	21 de septiembre 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 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 está siendo difundida a través de un correo electrónico supuestamente proveniente del Banco Ripley.

Con este phishing, el atacante busca persuadir a las personas de que hagan clic en un enlace adjunto en el cuerpo del correo. Para ello, el mensaje del email señala falsamente que la tarjeta del receptor ha sido bloqueada y que por ello deben acceder al enlace adjunto. De hacerlo, las personas son dirigidas a un sitio falso, donde se exponen al robo de sus datos confidenciales.

Observación

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

Indicadores de compromiso

URL redirección:
https://bit[.]ly/39zIwF7?l=www.bancoripley.cl

URL sitio falso:
http://www-bancoripleycl.eait.co[.]za/login

Asunto:
Fwd:Avios Importante - TarjetaRipley Bloqueada.

Correo electrónico
www-data@h2929933.stratoserver.net

SMTP Host
[81.169.236.156]

Otros antecedentes

Certificado Digital

Fecha Valido	:	NO APLICA
Fecha Término	:	NO APLICA
Emitido	:	NO APLICA

Datos Alojamiento

IP	:	[102.64.32.30]
Número de sistema autónomo (AS)	:	327991
Etiqueta del sistema autónomo	:	MEGASURF-WIRELESS-INTERNET
País	:	ZA
Registrador	:	AFRINIC

Datos del Dominio

Nombre de dominio	:	eait.co[.]za
Creado	:	25-06-2011
Expira	:	25-06-2022
Información del registrador	:	Domains
ID IANA	:	1645
Correo electrónico	:	abuse@domains.co.za
Servidores de nombres	:	ns1.deskpublish.com ns2.deskpublish.com

Imagen del mensaje

Fwd:Avios Importante - TarjetaRipley Bloqueada.

B BancoRipley <mensajeria@mensajeriaripley.cl>
Lun 20-09-2021 20:44
Para: Usted

BancoRipley,le informa que su cuenta muestra un mensaje de Error: RUS 00748-206, mismo que se define como TARJETA BLOQUEADA, este codigo se ah generado porque usted no culmino con el proceso de verificacion de Identidad(email y telefono).

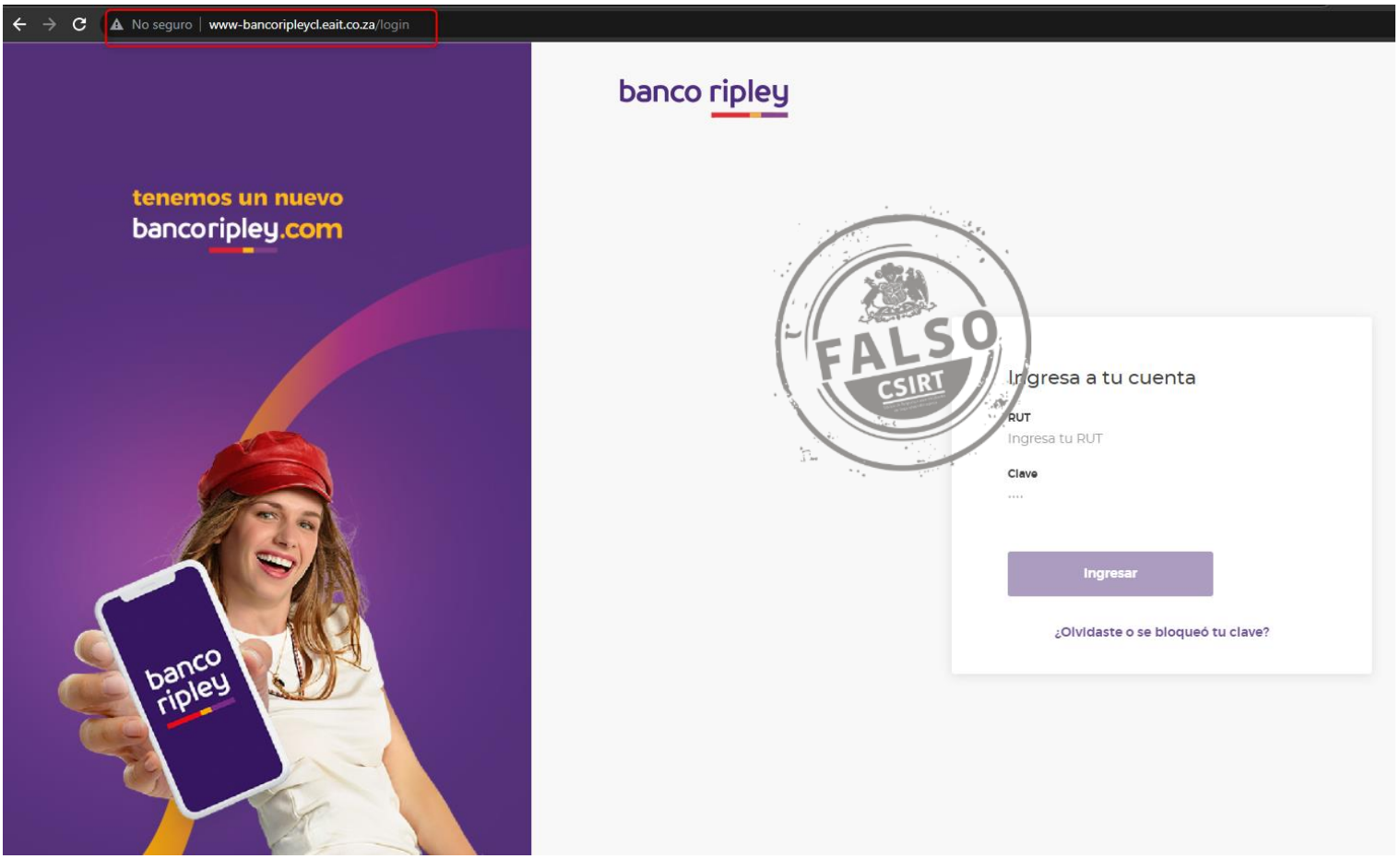
Es necesario que ingrese a nuestra web para poder verificar su informacion en nuestra base de datos o de lo contrario su servicio de banca por internet quedara BLOQUEADA y sera necesario acudir a nuestra sucursal mas cercana para el desbloqueo de su cuenta.

Valida tu Identidad,CONFIRMA TU DATOS y listo!

Ingresa aqui

Si tienes consultas o deseas mas informacion en su banco o en www.bancoripley.cl

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: 2021.09.22 10:13:19 -03'00'