Alerta de seguridad informática	8FPH22-00516-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2022
Última revisión	25 de abril de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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) ha identificado una campaña de phishing vía correo electrónico que proviene, supuestamente, del Banco Ripley. En esta campaña, los delincuentes indican falsamente a la víctima que tiene un monto aprobado por $1.000.000. Para ello, debe solicitarlo en un enlace que dispone el atacante en el correo. Al ingresar, la persona es dirigida a un sitio falso, semejante al Banco Ripley, donde se expone al robo de su usuario y contraseña (credenciales).

Observación

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

Indicadores de compromiso

URL redirección:
hXXps://bit[.]ly/3v1ErVC?l=www.bancoripley.cl
hXXps://www.clmedicalltd[.]com/wp-content/languages/plugins/enviar.php?l=666704876
hXXps://wardatalwadirealestates[.]com/activacion/cuenta-ljei/

Sitio falso:
hXXp://www-bancoripley.cl.workhost[.]in/1650898777/login

Asunto:
Fwd: Aviso, Tienes Credito Aprobado no te pierdas esta oportunidad unica.

Correo de salida:
web341@srv042044.webreus.net

SMTP Host:
[46.235.47.4]

Otros antecedentes

Certificado Digital

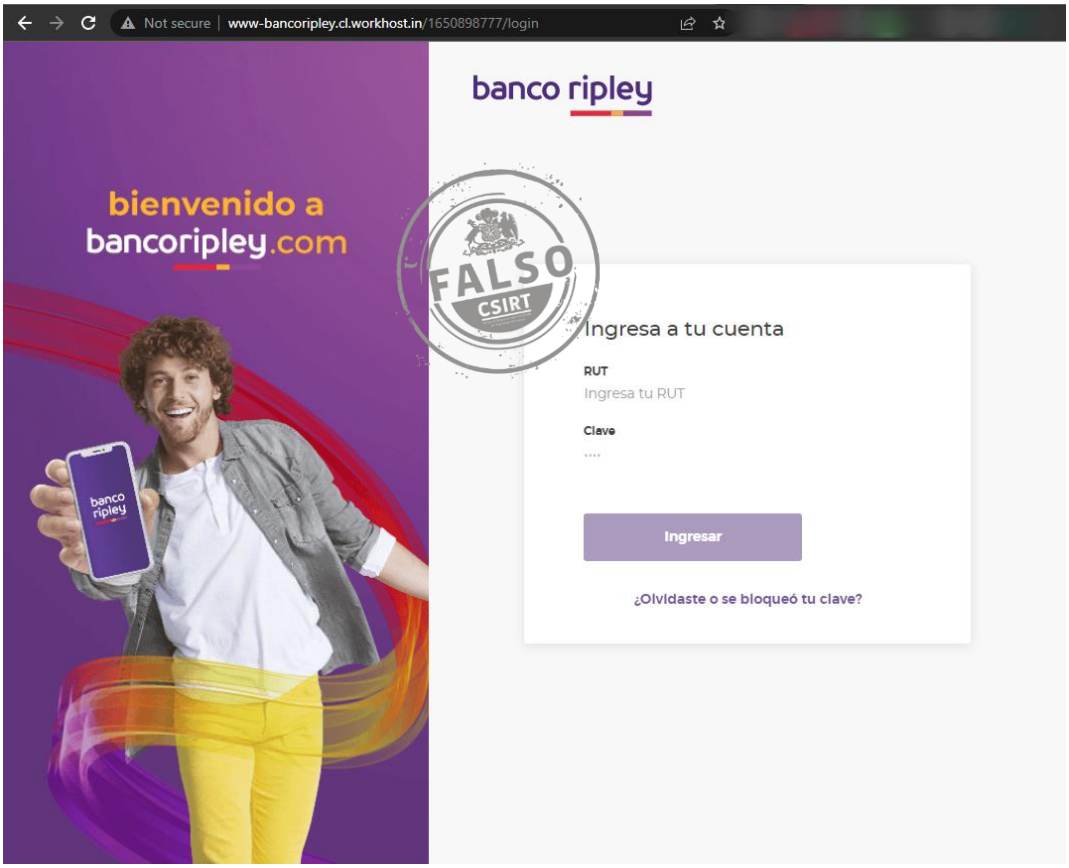
Fecha Válido	:	11-04-2022
Fecha Término	:	10-07-2022
Emitido	:	Let's Encrypt R3

Datos Alojamiento y Dominio

IP	:	[94.130.8.49]
Número de sistema autónomo (AS) IP	:	24940
Etiqueta del sistema autónomo IP	:	Hetzner Online GmbH
Registrador IP	:	RIPE NCC
País IP	:	DE
Dominio	:	www-bancoripley.cl.workhost[.]in
Registrador Dominio	:	GoDaddy.com, LLC

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: 2022.04.25 12:26:18 -04'00'