Alerta de seguridad informática	8FPH21-00446-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de noviembre de 2021
Última revisión	22 de noviembre 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 se está difundiendo a través de un correo electrónico que dice falsamente provenir del Banco Ripley.

Con este email, el atacante busca persuadir a las personas de utilizar un enlace adjunto en el cuerpo del correo, el cual indica falsamente que el banco se ha adherido al programa de ayuda del Gobierno “Línea Covid 19”, por lo que se supuestamente encuentra aprobado un crédito.

De ingresar a los enlaces disponibles, las víctimas 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

Urls redirección:
http://yashevents.co[.]in/ganador/promo-riwc/

Urls sitio falso:
https://blogs.neloz[.]cl/login

Asunto:
✓ Notificación: Crédito Aprobado

Correo Electrónico:
noreply@publimailer.com

SMTP Host:
[170.239.85.224]

Otros antecedentes

Certificado Digital

Fecha Válido	:	31-10-2021
Fecha Término	:	30-01-2021
Emitido	:	Panel, Inc. Certification Authority

Datos Alojamiento

IP	:	[200.63.99.33]
Número de sistema autónomo (AS)	:	265831
Etiqueta del sistema autónomo	:	SOC. COMERCIAL WIRENET CHILE LTDA.
País	:	CL
Registrador	:	LACNIC

Datos del Dominio

Nombre de dominio	:	neloz[.]cl
Creado	:	11-07-2016
Expira	:	11-07-2022
Información del registrador	:	NIC Chile
ID IANA	:	NO APLICA
Correo electrónico	:	NO APLICA
Servidores de nombres	:	ns.hostingtop.cl ns.vinculos.cl

Imagen del mensaje

✓ Notificacion: Credito Aprobado

B BancoRipley <noreply@publimailer.com>
Jue 18-11-2021 10:54
Para: Usted

banco ripley

OPERA SEGURO ✓Siempre

Estimado(a): on @hotmail.com

FALSO CSIRT

BancoRipley. En su permanente interes por apoyar a sus clientes, ha adherido al programa del gobierno denominado Linea Covid-19.

Su credito fue aprobado por el comite del banco por el Plazo de 24 a 48 meses y 6 meses de gracia. Para sus necesidades financieras. Asi no tendras que salir de casa.

Revisa tu credito por este E-mail. Aqui

Si tienes consultas o deseas mas informacion, ingresa aqui:

Activar Credito

OPERACION REALIZADA

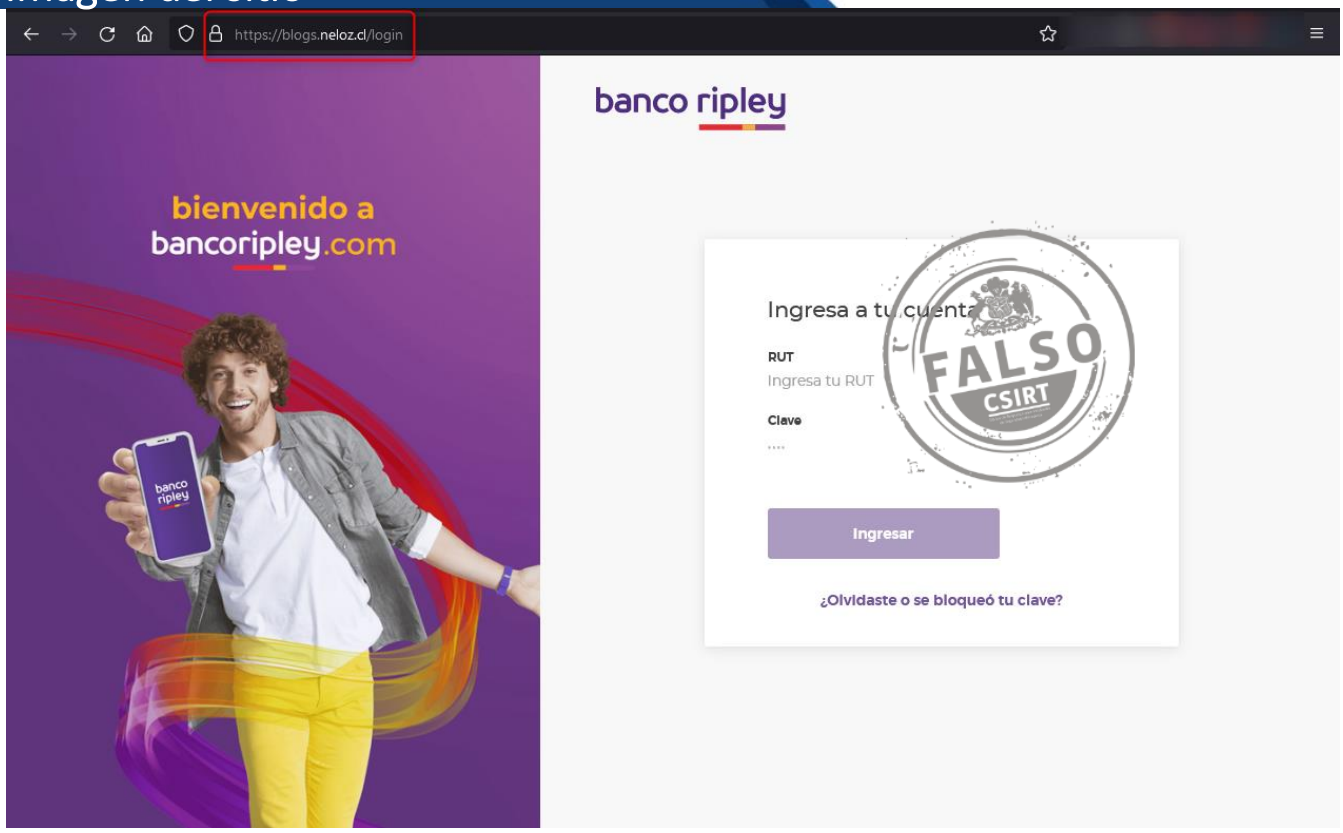
https://web.bancoripley.cl/login

Lamentamos las molestias que esta situacion pueda ocasionar.

Si no deseas continuar recibiendo correos de BancoRipley, por favor haz **click aqui**

Responder | Reenviar

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.