Alerta de seguridad informática	8FPH21-00394-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de abril de 2021
Última revisión	21 de abril 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 mensajería que supuestamente proviene desde la empresa Ripley.

El atacante busca persuadir a las personas para utilizar un enlace adjunto en el cuerpo del mensaje. El mensaje indica al usuario: “el Banco Ripley informa que su tarjeta Ripley está Bloqueada”. Al seleccionar el enlace para supuestamente desbloquear su tarjeta, las personas son dirigidas a un sitio falso, donde se exponen al robo de sus credenciales.

Observación

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

Indicadores de compromiso

URL sitio redirección:
https://bit[.]ly/3uYUsJ0?l=www.bancoripley.cl
http://terrasplaceaz[.]com/wp-content/mu-plugins/enviar02.php?l=1842395817
https://bit[.]ly/3n1O3di?l=www.bancoripley.cl
https://ironguard[.]ro/activacion/cuenta-jlaj/

URL sitio falso:
wwwbancoripley.cl.asthamart[.]com/

Asunto:
TarjetaRipley BLOQUEADA

Correo electrónico
info@ebikebrandstore[.]nl

Servidor SMTP
[88.99.251.31 - production932.hipex.io]

Otros antecedentes

Certificado digital

Fecha Valido	:	No aplica
Fecha Término	:	No aplica
Emitido	:	No aplica

Datos alojamiento

IP	:	[162.213.196.78]
Número de sistema autónomo (AS)	:	54540
Etiqueta del sistema autónomo	:	INCERO-HVVC
País	:	US
Registrador	:	ARIN

Datos del dominio

Nombre de dominio	:	asthamart[.]com
Creado	:	06-12-2017
Expira	:	06-12-2021
Información del registrador	:	SHEIKH SADIK SHAHRIYAR
ID IANA	:	1229
Correo electrónico	:	niloy81@yahoo.com
Servidores de nombres	:	ns1.digitechvalley.com ns2.digitechvalley.com

Imagen del mensaje

banco ripley

Estimado(a):

Banco Ripley, le informamos que su **Tarjeta Ripley esta BLOQUEADA**, el bloqueo se realizo por que nuestro sistema de seguridad detecto compras en el extranjero y operaciones que no son habituales en su cuenta, necesita activar su **Tarjeta Ripley para poder ingresar a su banca por internet.**

Para solucionar este inconvenientes,

Ingrese.Aqui

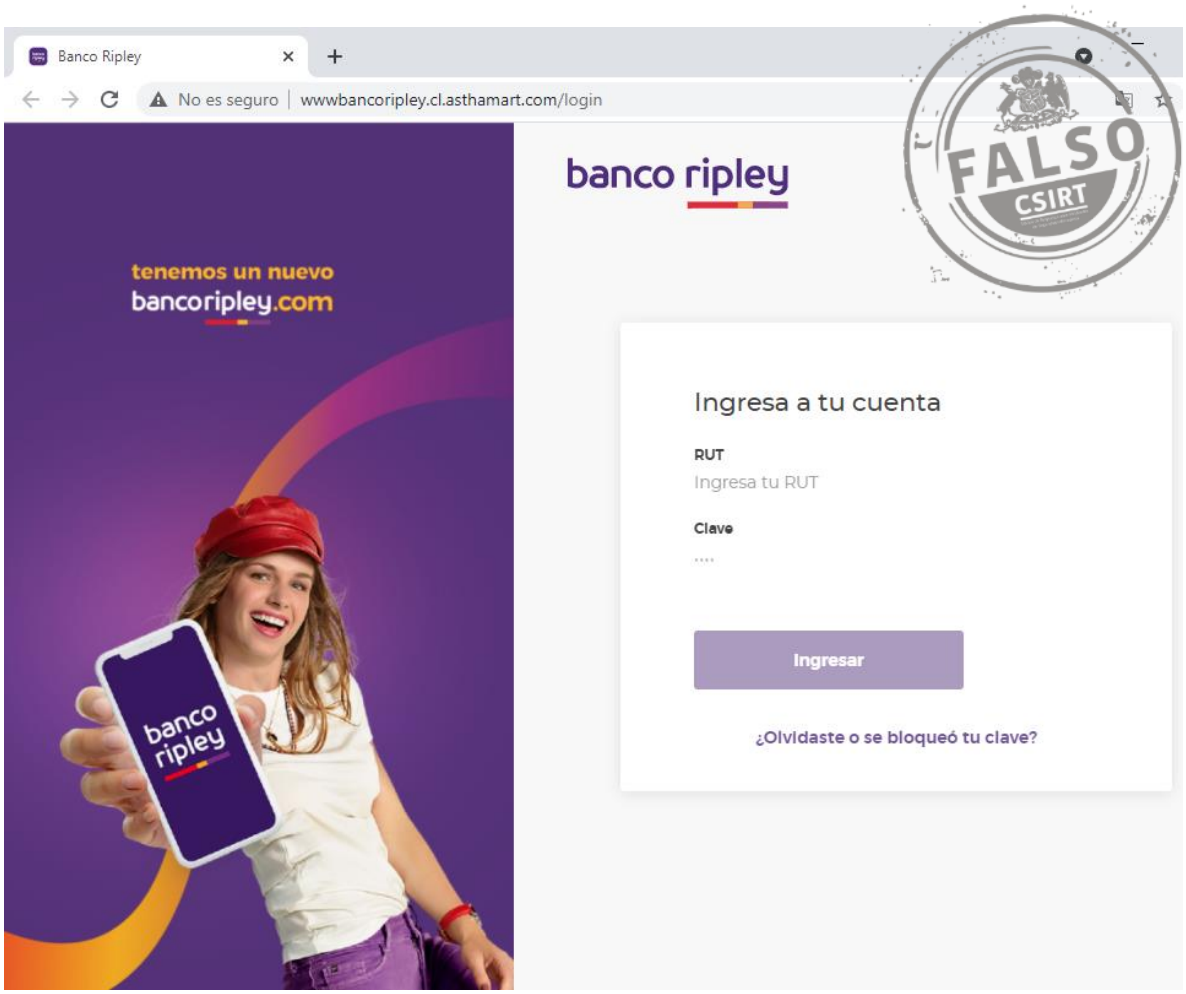
FALSO CSIRT

Si tienes consultas o deseas mas informacion:

www.bancoripley.cl

Atentamente, BancoRipley.

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: 2021.04.21 20:52:55 -04'00'