Alerta de seguridad cibernética	8FPH21-00437-01
Clase de alerta	Fraude
Tipo de incidente	smishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de octubre de 2021
Última revisión	05 de octubre 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 smishing que se está difundiendo, que se hace pasar como proveniente del Banco de Chile.

Para engañar al receptor, el mensaje indica falsamente que “el dispositivo MIPASS se encuentra inactivo”, dejando un link para que la víctima haga clic en el enlace adjunto en el mensaje de texto. De seleccionar el link, la víctima es dirigida a un sitio falso, donde se expone al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Texto Mensaje:
Banco de Chile: Estimado Cliente su dispositivo MIPASS se encuentra INACTIVO. Realice proceso de verificación. Piche aquí.

Urls de SMS:
https://bitly[.]com/3trinkD

Urls sitio falso:
http://139.59.88[.]100/1633348621/bcochile-web/persona/login/index.html/login

Otros antecedentes

Certificado Digital

Fecha Valido	:	No aplica
Fecha Termino	:	No aplica
Emitido	:	No aplica

Datos Alojamiento

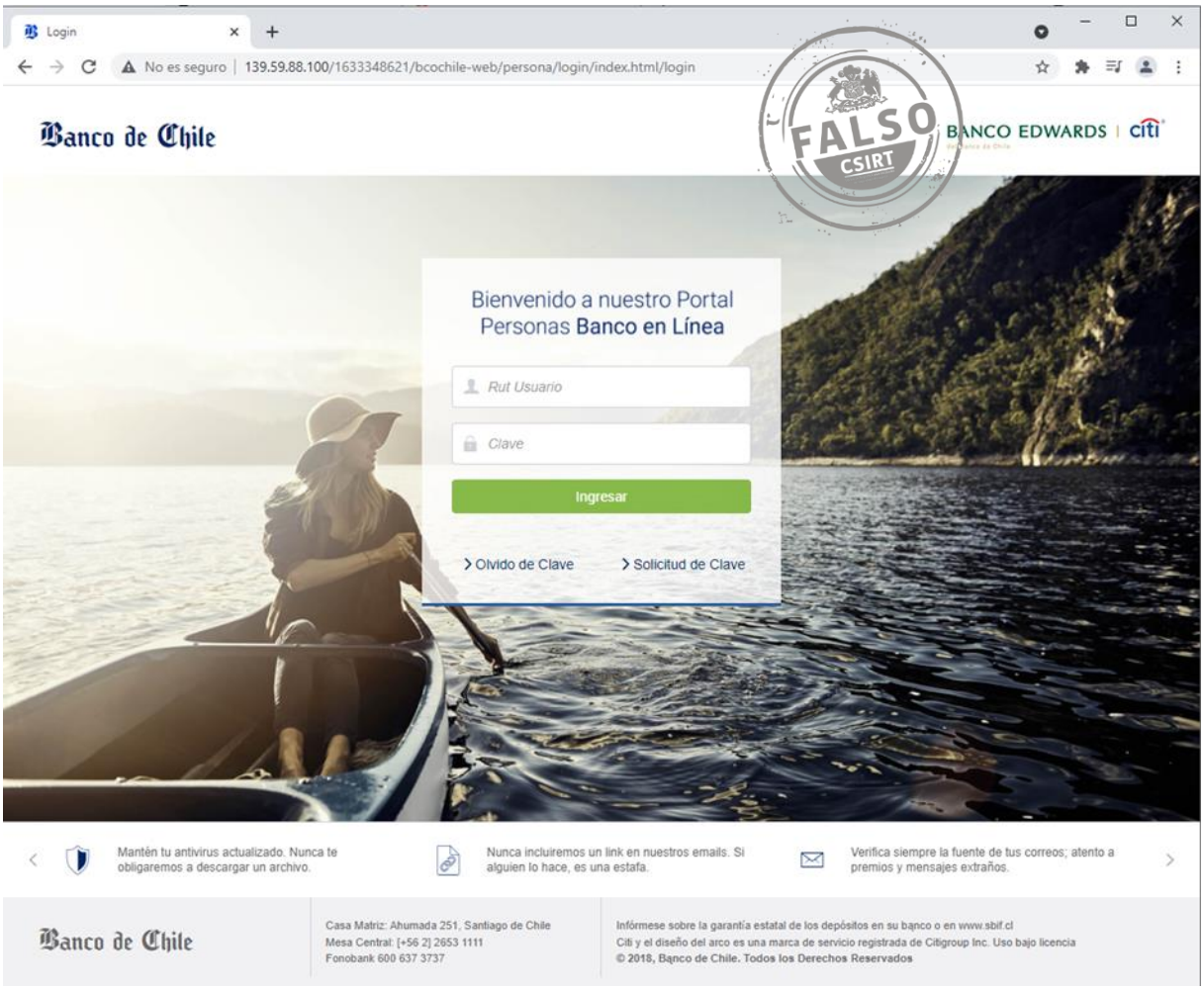
IP	:	[139.59.88.100]
Número de sistema autónomo (AS)	:	14061
Etiqueta del sistema autónomo	:	DIGITALOCEAN-ASN
País	:	IS
Registrador	:	APNIC

Datos del Dominio

Nombre de dominio	:	139.59.88.100
Creado	:	No aplica
Expira	:	No aplica
Información del registrador	:	No aplica
ID IANA	:	No aplica
Correo electrónico	:	No aplica
Servidores de nombres	:	No aplica
		No aplica

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: 2021.10.05 15:44:39 -03'00'