Alerta de seguridad informática	8FPH22-00549-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de junio de 2022
Última revisión	29 de junio de 2022

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) ha identificado una campaña de phishing vía correo electrónico que proviene, supuestamente, del Banco de Chile. En esta campaña, los delincuentes indican falsamente a la víctima que se ha intentado un ingreso desde un dispositivo desconocido a su cuenta de banco, por lo que se ha restringido el acceso a la banca temporalmente. Para restablecer el acceso, el atacante dispone de un enlace, el cual dirige a un sitio falso, semejante al Banco de Chile, 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:
https://bit[.]ly/3NbCsUs
https://gocloudasiaacademe[.]com/?id=231

Sitio falso:
https://login.portal.bancochlle.cl.iranorganic[.]org/

Asunto:
Servicio suspendido.

Correo de salida:
gdl1@microclick[.]com.mx
mjrivera@pcl[.]mx
gdl1@microclick[.]com.mx
mjrivera@pcl[.]mx

SMTP Host:
[98.142.111.77]
[168.195.204.51]
[98.142.111.77]
[168.195.204.51]

Otros antecedentes

Certificado Digital

Fecha Válido	:	27-06-2022
Fecha Término	:	25-09-2022
Emitido	:	Let's Encrypt R3

Datos Alojamiento y Dominio

IP	:	[89.38.97.213]
Número de sistema autónomo (AS) IP	:	49981
Etiqueta del sistema autónomo IP	:	WorldStream B.V.
Registrador IP	:	RIPE NCC
País IP	:	NL
Dominio	:	iranorganic[.]org
Registrador Dominio	:	Tucows Domains Inc.

Imagen del mensaje

Servicio suspendido.

S serviciodeseguridad@bancochile.cl <gdl1@microclick.com.mx>
Para

Responder | Responder a todos | Reenviar | ...
miércoles 29-06-2022 9:48

Banco de Chile

FALSO CSIRT

Actividad Sospechoza

Estimado(a),
Hemos detectado que se ha intentado un ingerso desde un dispositivo desconocido a su cuenta de banco por lo que hemos restringido el acceso a su banca temporalmente.

Para restablecer el acceso, ingrese al portal en el siguiente enlace.

Restablecer

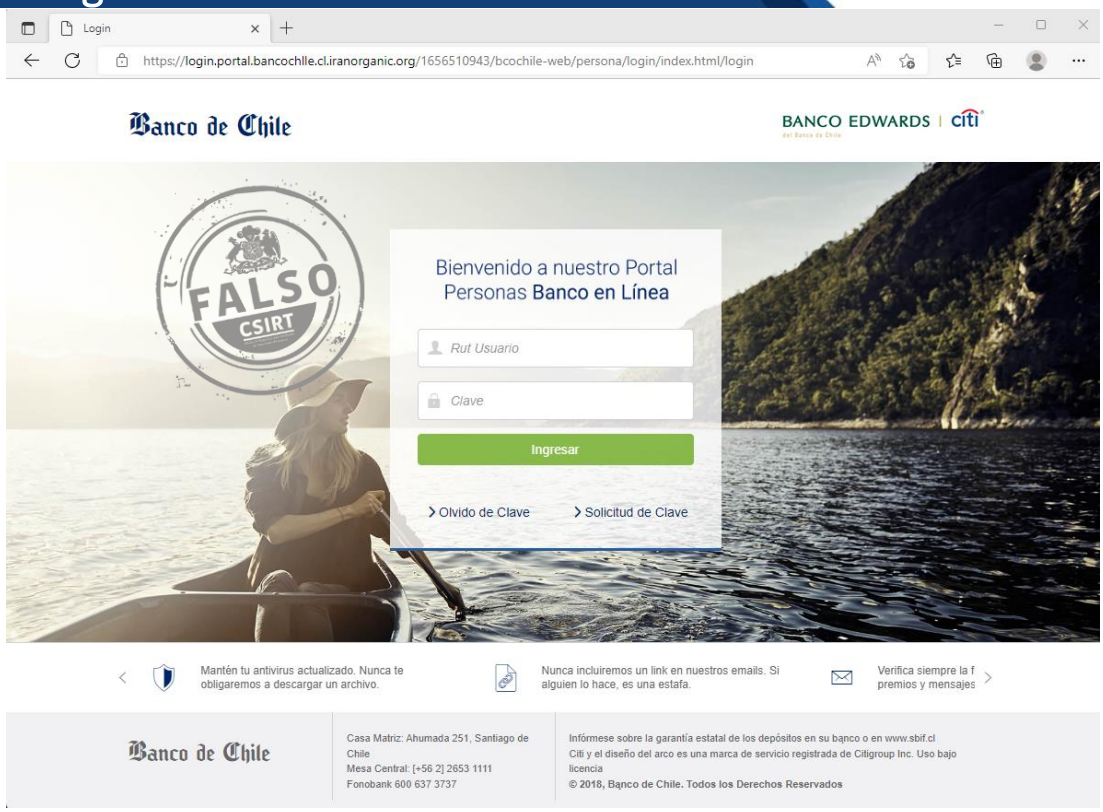
Atte Banco de Chile.

Código:
CWG49626628533171888932

Fecha y Hora:
Lunes 27 de junio de 2022 20:23

Infórmese sobre la garantía estatal de los depósitos en su banco o en www.cmfchile.cl
2022 Banco de Chile. Todos los Derechos Reservados.

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: 2022.06.29 10:49:38 -04'00'