Alerta de Seguridad Informática (8FPH-00029-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 17 de Junio de 2019 | Última revisión 17 de Junio de 2019

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.

Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), en colaboración con el Departamento de Tecnologías de la Información del Servicio Agrícola y Ganadero, han identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco de Chile. El correo trata de persuadir a los clientes para que actualicen sus datos y ofrecen como incentivo $500.000 mil pesos, lo que serían supuestamente depositados de forma automática con la actualización de los datos. Adicionalmente, los clientes reciben un segundo estímulo, el de estar participando en un sorteo de 30 ipads mini, 20 televisores 4k, entre otros. Bajo las premisas anteriores, los delincuentes intentan convencer a sus víctimas para que accedan a un enlace malicioso ubicado en el correo y de esta forma, entregar las credenciales de acceso de la cuenta bancarias.

Indicadores de compromisos

Url's:

http[:]//www[.]webportal[.]dns04[.]com

http[:]//www[.]webportal[.]world/local/bancochile/wps/wcm/connect/Personas/Portal/public/cliente

Smtp Host

[85.143.222.27] choff001.manage-smtpbz[.]pro
[85.143.220.247] choff002.manage-smtpbz[.]pro

Server[.]socialmediaconsultingcfl[.]com [163.172.107.56]

From: (Suplantación de cuentas)

enviodigital@socofin.cl
newsletter@eeccvirtual.cl

Subject:

Banco de Chile te premia con $ 500,00 pesos

Imágenes

Banco de Chile <enviodigital@socofin.cl>
Banco de Chile te premia con $ 500,000
Haga clic aquí para descargar imágenes. Para ayudarle a proteger su confidencialidad, Outlook ha impedido la descarga automática de algunas imágenes en este mensaje.

Si no visualiza el correo completo haga clic en Mostrar Contenido Bloqueado

Este correo se a enviado para:

Banco de Chile

Disfruta de los mejores beneficios con tus tarjetas de credito de Banco de Chile.

ESTIMADO CLIENTE:

Mastercard y Banco de Chile te premian con $ 500.000 mil pesos en tu linea de credito, para que los gastes en lo que desees, solo actualiza tus datos y automaticamente se debitara en su cuenta el monto indicado. Tambien entraras al sorteo de 30 ipads mini, 20 televisores 4k para que disfrutes viendo tu serie o pelicula favorita, paquetes dobles para una cena romantica y cientos de cientos de premios mas.

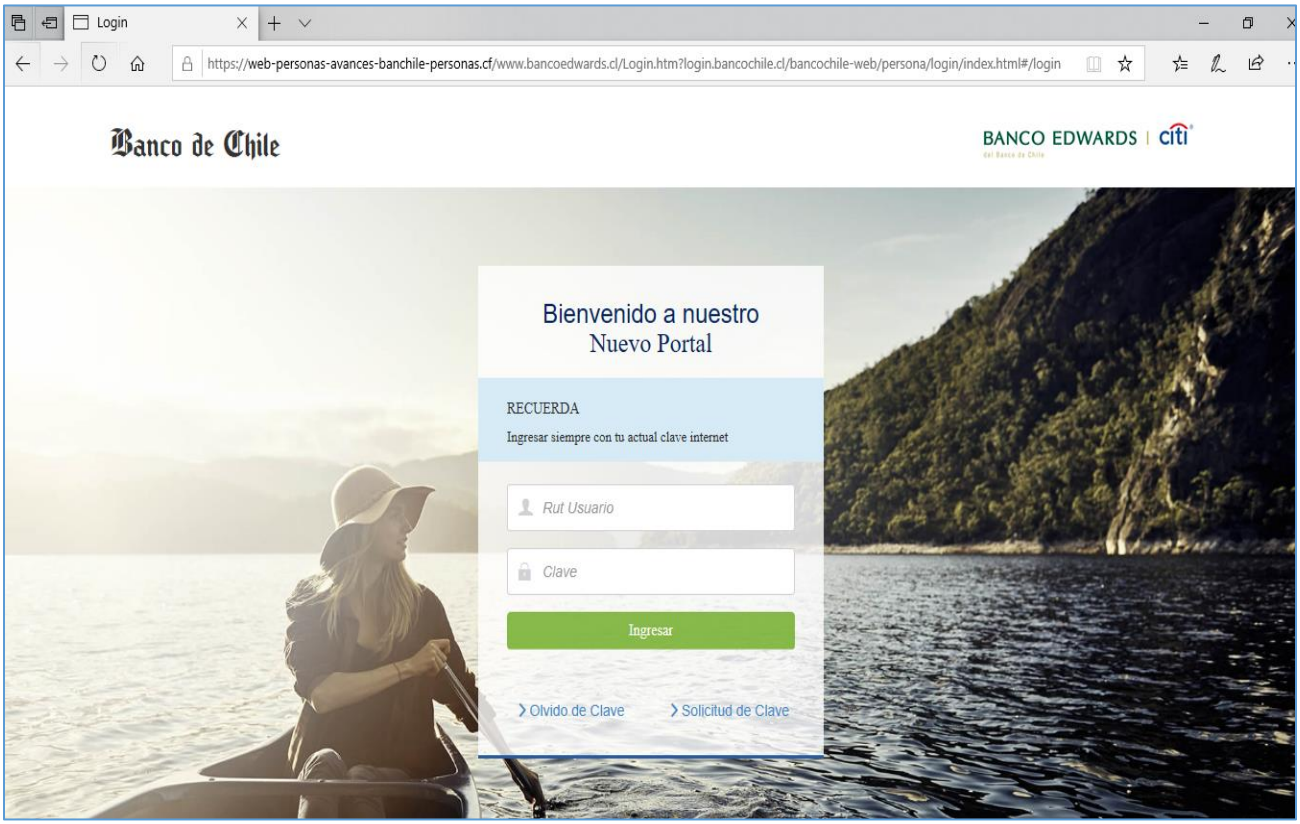
El sorteo se llevara a cabo los dias 15 de cada mes y sera publicado en nuestra pagina web, los ganadores seran notificados con una llamada por uno de nuestros ejecutivos debidamente identificados.

Quieres aprobar los $ 500,000 ingrese al siguiente link

Actualizar mis datos

Las tildes fueron omitidas intencionalmente
Este corre electronico se le envio a

Casa Matriz: Ahumada 251, Santiago de Chile


Login
https://web-personas-avances-banchile-personas.cf/www.bancoedwards.cl/Login.htm?login.bancochile.cl/bancochile-web/persona/login/index.html#/login
Banco de Chile
BANCO EDWARDS | citi
Bienvenido a nuestro
Nuevo Portal
RECUERDA
Ingresar siempre con tu actual clave internet
Rut Usuario
Clave
Ingresar
Olvido de Clave
Solicitud de Clave

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob