Alerta de Seguridad Informática (8FPH-00024-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 27 de Mayo de 2019 | Última revisión 27 de Mayo 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), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Chile. El correo trata de persuadir a los clientes informándoles de un supuesto aumento de cupo en su Línea de Crédito, al que puede acceder ingresando a través del link adjunto. Adicionalmente, en el correo tratan de aumentar el interés del usuario indicándoles que pueden ganar diferentes premios en un supuesto sorteo (60 LED Samsung de 55' - 100 PLAY STATION 4 - 250 IPHONE 6 PLUS 126GB).

Indicadores de compromisos

Url's:

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

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

http[:]//www[.]personasweb[.]site/bancochile/wps/wcm/connect1/Personas1/Portalpersonas1/58z77tkqra/juif8_persona/login_wy4y/index/loginbiwe/

Smtp Host

115-34-44-64-.reverse-dns [64.44.34.115]

From:

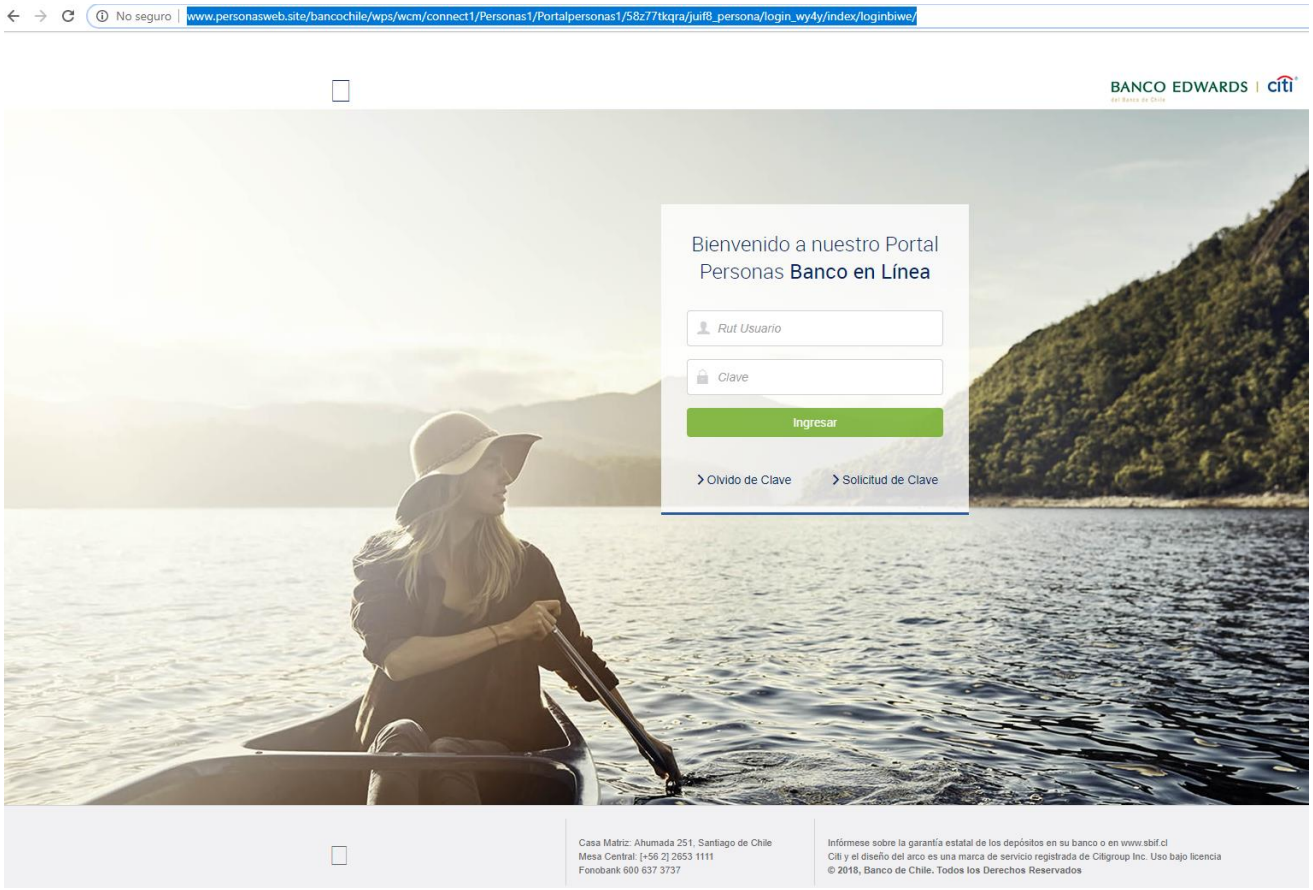
admin@tradicionesverdes.com

Subject:

Tienes aprobado $ 784.033 a su linea de credito

Imagen


Banco de Chile <enviodigital@bancochile.ch>
Tienes aprobado $ 784.033 a su linea de crédito...
Datos adjuntos sin título 00019.txt
139 bytes
Si no visualiza el correo completo haga clic en Mostrar Contenido Bloqueado
Este correo se a enviado para:
Banco de Chile
Banco de Chile tiene las mejores opciones en servicios bancarios en linea, cuenta corriente, pago con tarjeta de credito, credito hipotecario.
ESTIMADO CLIENTE:
Para eso que tienes pensado GANA$TE un cupo en tu linea de credito de $ 784.033, usalo en lo mejor que te parezca. Al aumentar el cupo en tu Linea de Credito ingresaste automaticamente tambien al sorteo de 60 televisores LED Samsung de 55' - 100 PLAY STATION 4 - 250 IPHONE 6 PLUS 126GB
Para Aprobar su abono de $ 784,033 ingrese al siguiente link
Abonar Linea de Credito
Las tildes fueron omitidas intencionalmente
Este corre electronico se le envio a exonerados@interior.gov.cl
Casa Matriz: Ahumada 251, Santiago de Chile


No seguro
www.personasweb.site/bancochile/wps/wcm/connect1/Personas1/Portalpersonas1/58z77tkqra/juif8_persona/login_wy4y/index/loginbiwe/
BANCO EDWARDS | citi
Bienvenido a nuestro Portal
Personas Banco en Línea
Rut Usuario
Clave
Ingresar
Olvido de Clave
Solicitud de Clave
Casa Matriz: Ahumada 251, Santiago de Chile
Mesa Central: [+56 2] 2653 1111
Fonobank 600 637 3737
Infórmese sobre la garantía estatal de los depósitos en su banco o en www.sbif.cl
Citi y el diseño del arco es una marca de servicio registrada de Citigroup Inc. Uso bajo licencia
© 2018, Banco de Chile. Todos los Derechos Reservados

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre 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