Alerta de Seguridad Informática (8FPH-00047-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 23 de Julio de 2019 | Última revisión 23 de Julio 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. Los correos intentan engañar a los usuarios indicando que el dispositivo digipass que posee debe ser sincronizado por internet. El mensaje intenta persuadir a la potencial víctima enfatizando que la operación es necesaria para poder ingresar a su cuenta en línea y así beneficiarse de los servicios que ofrece el banco. Para ejercer aún más presión en la decisión del usuario, el mensaje advierte al usuario que "solo tiene 48 horas para poder realizar este proceso mediante el enlace brindado, de lo contrario la cuenta será inhabilitada". De este modo, el atacante intenta de convencer al usuario para ingresar al enlace y entregar sus credenciales en un sitio semejante al del banco.

> "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"

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

- http[:]//greenchildproject[.]com/a1204aa5a605965b1ff09c397dcf1bee/
- http[:]//portalbedexchile[.]solumbyerd[.]com/wkmui8q8bs/38sfn_prsona/lgin_2vhj/jzb93v/loginrl6x

Smtp Host

- 19ceb.l.time4vps.cloud [89.40.15.52]
- 19bfb.l.time4vps.cloud [194.135.95.170]
- 19cee.l.time4vps.cloud [212.24.102.72]
- 19ce9.l.time4vps.cloud [109.235.65.36]
- 19ced.l.time4vps.cloud [94.176.239.28]
- 19cea.l.time4vps.cloud [212.24.109.58]

From:

- root@19ceb.l.time4vps.cloud
- root@19bfb.l.time4vps.cloud
- root@19cee.l.time4vps.cloud
- root@19ce9.l.time4vps.cloud
- root@19ced.l.time4vps.cloud
- root@19cea.l.time4vps.cloud

Subject:

- Sujeto a bloqueo si no sincroniza su digipass.

Imagen Phishing correo

Banco de Chile <enviosdigital@bancochile.cl>

✓ Sujeto a bloqueo si no sincroniza su digipass.

Banco de Chile

El banco de Chile

Si no puede ver el email de clic aqui por favor.

Estimado Cliente:

Banco de Chile necesita sincronizar su digipass registrado en nuesta banca por internet, esta operacion requiere ser atendida para poder ingresar a sus cuentas afiliadas a Banco En Linea y empezar a gozar de los beneficios que nuestra plataforma le ofrece.

Recuerde que solo tiene 48 horas despues de haber recibido este correo para realizar este proceso mediante el enlace brindado, de lo contrario su cuenta sera inhabilitada y tendra que acercarse a la sucursal mas cercana para solicitar una nueva tarjeta.

Digipass	Estado de Registro	**No Sincronizado**

Sincronizar Aquí

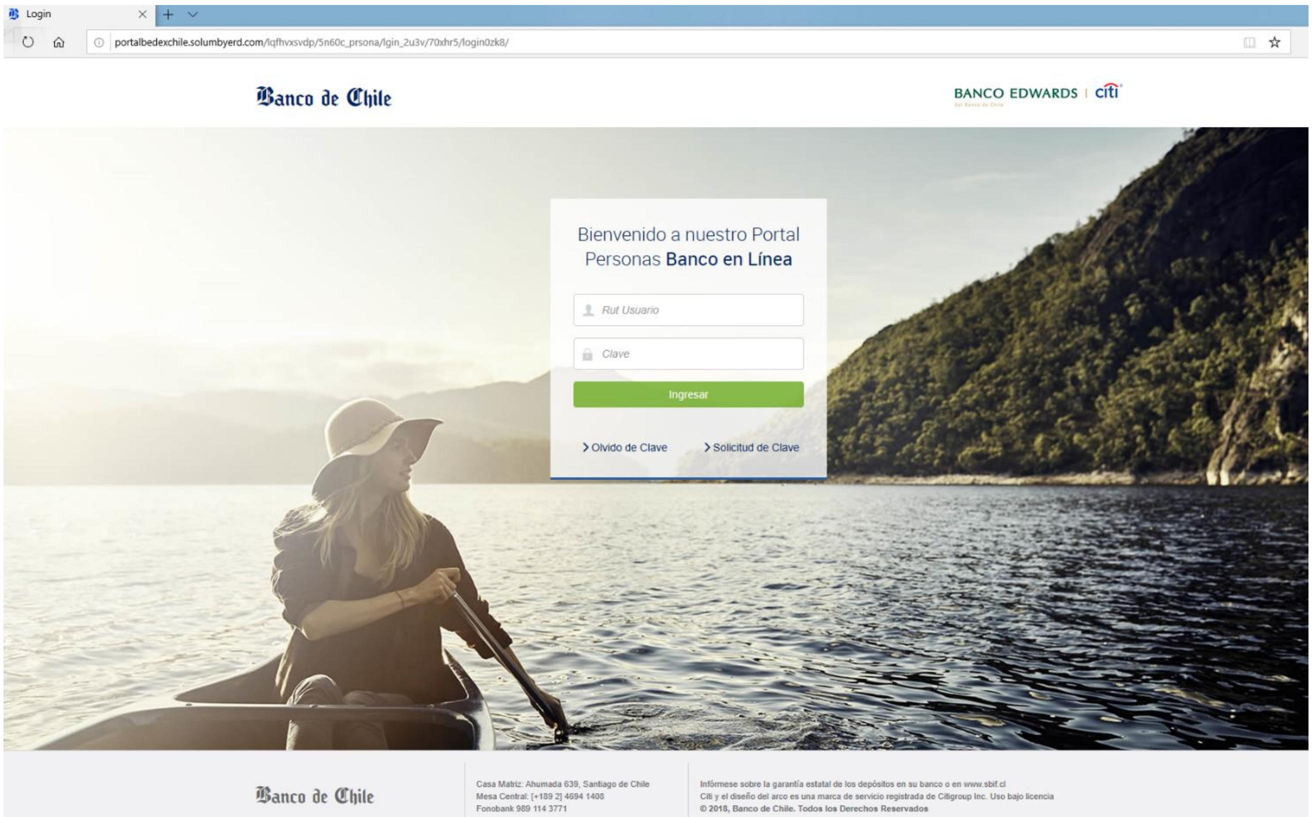
http://ww3.bancochile.cl/personas/

Por confiar en nosotros le damos las gracias.

Atentamente: Servicio al cliente, Banco de Chile

Banco de Chile es el emisor de la tarjeta de crédito Travel Club, Club La Tercera Visa y Entel Visa, siendo el prestador de los servicios bancarios asociados a estas.
Infórmese sobre la garantía estatal de los depósitos en su banco o en www.sbif.cl
© 2015 Banco de Chile. Todos los Derechos Reservados.

Imagen Sitio Web



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
- Visualizar los sitios web que se ingresen que sean los oficiales

Contactos

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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.23 17:51:26 -04'00'