Alerta de seguridad informática	**8FPH-00054-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Phishing**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**06 de Agosto de 2019**
Última revisión	**06 de Agosto 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.

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), con la colaboración de usuarios de redes sociales[1], ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco Chile, solicitando a quienes pudieran recibir el correo que sincronicen su dispositivo DigiPass ya que existe un error, el cual se solucionaría con la sincronización, indicando que esta acción es “obligatoria”, de lo contrario la cuenta podría ser bloqueada por temas de seguridad. Si el usuario ingresa al enlace se expone a que el atacante robe sus credenciales desde un sitio semejante al del Banco.

[1] CSIRT destaca la colaboración de Juan López y Felipe Ovalle.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

https://www.cl-empresas[.]com/mobile/choose[.]php
https://www.cl-empresas[.]com/mobile/empresa/acesso[.]php
https://www.cl-empresas[.]com/mobile/empresa-2.0/acesso[.]php

Smtp Host

cac19[.]novaacaolivro[.]com[.]de [139.99.223.125]
sac3[.]novaacaolivro.com[.]de [51.83.225.55]

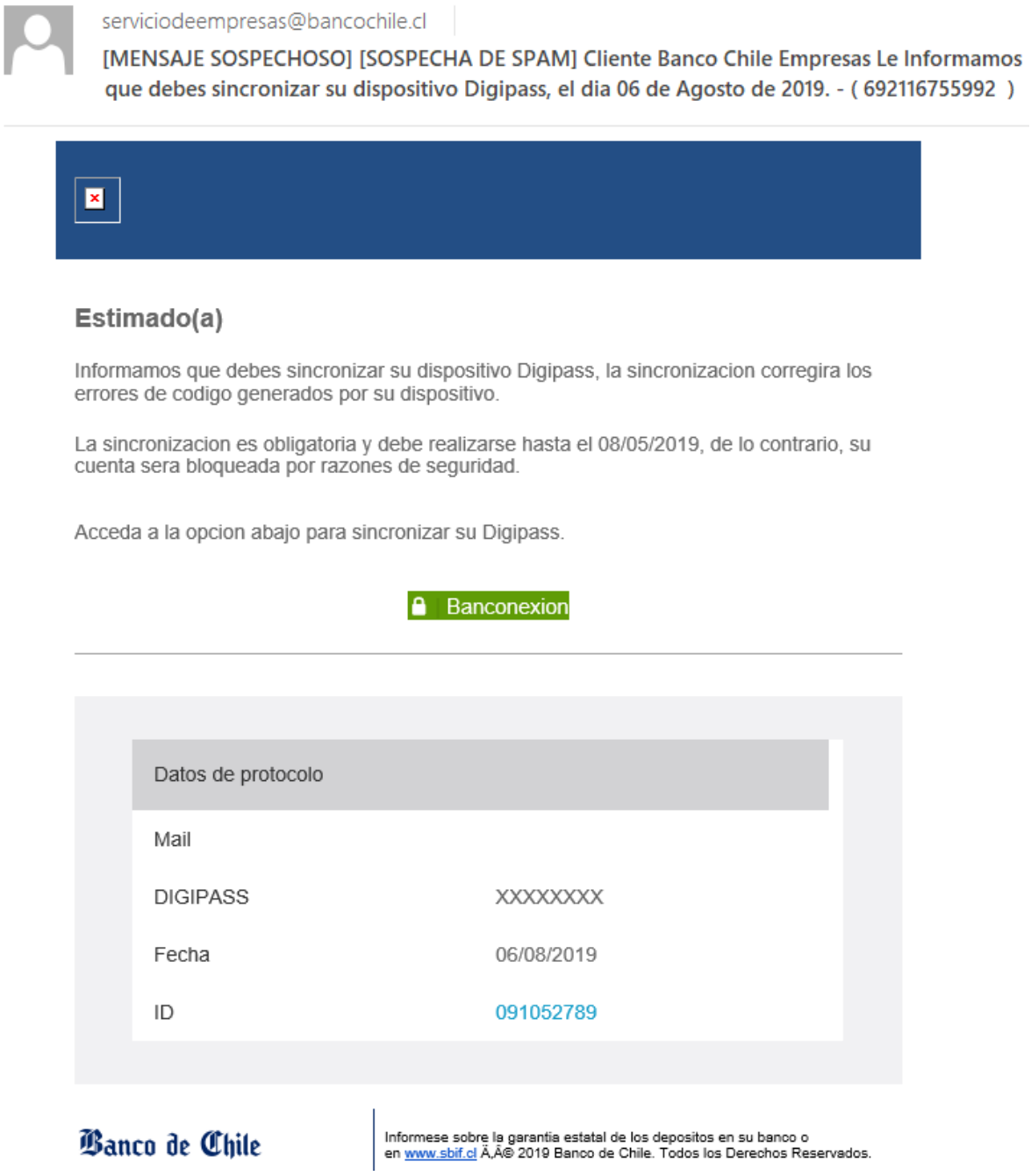
From:

apache@cac19[.]novaacaolivro[.]com[.]de
apache@cac17[.]novaacaolivro[.]com[.]de
apache@cac20[.]novaacaolivro[.]com[.]de
apache@sac3[.]novaacaolivro[.]com[.]de

Subject:

Cliente Banco Chile Empresas Le Informamos que debes sincronizar su dispositivo Digipass, el dia 06 de Agosto de 2019.

Imagen Phishing Correo



serviciodeempresas@bancochile.cl

[MENSAJE SOSPECHOSO] [SOSPECHA DE SPAM] Cliente Banco Chile Empresas Le Informamos que debes sincronizar su dispositivo Digipass, el dia 06 de Agosto de 2019. - (692116755992)

Estimado(a)

Informamos que debes sincronizar su dispositivo Digipass, la sincronizacion corregira los errores de codigo generados por su dispositivo.

La sincronizacion es obligatoria y debe realizarse hasta el 08/05/2019, de lo contrario, su cuenta sera bloqueada por razones de seguridad.

Acceda a la opcion abajo para sincronizar su Digipass.

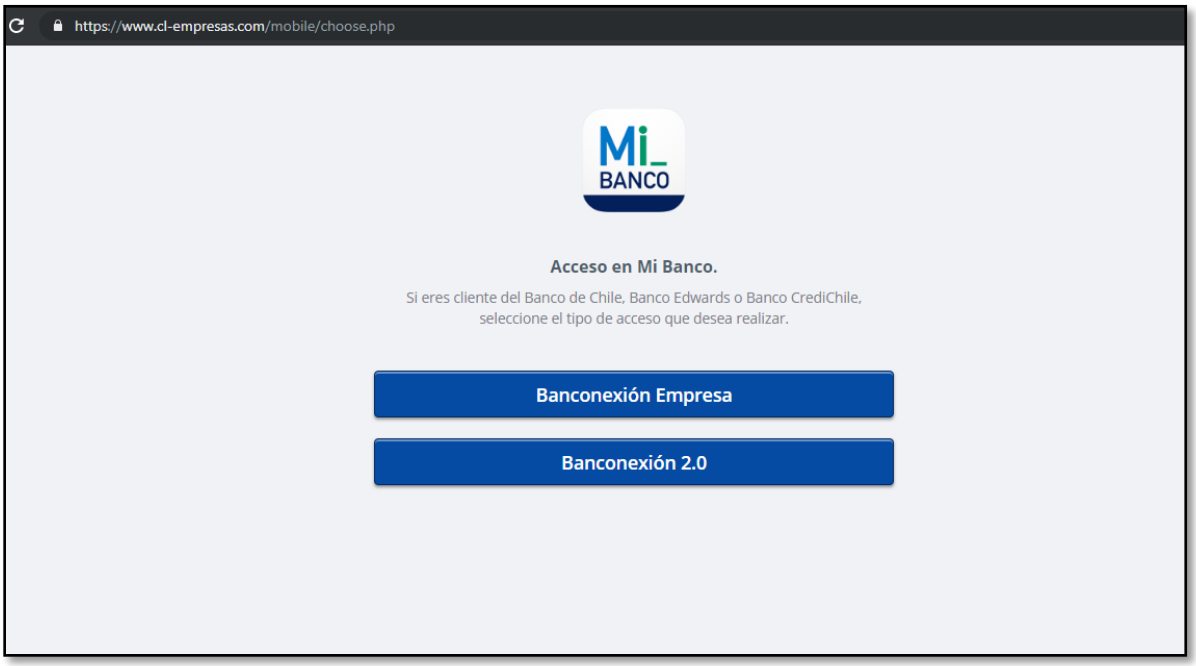
Banconexion

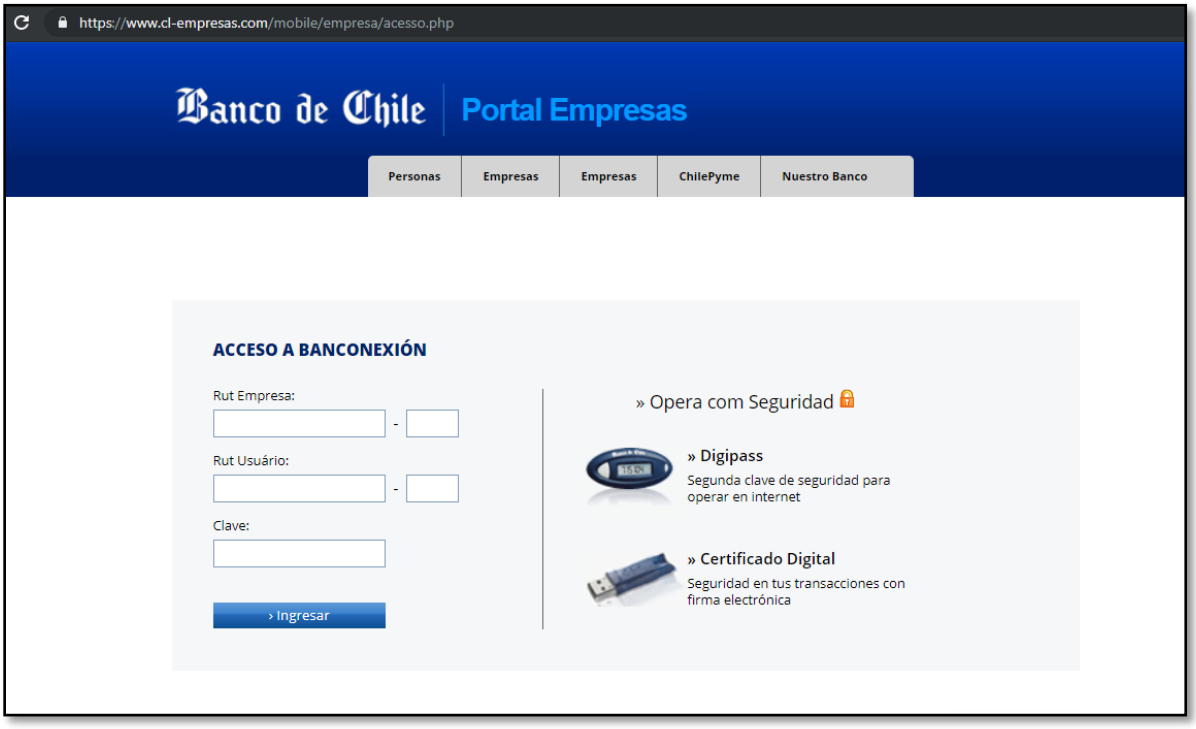
Datos de protocolo	
Mail	
DIGIPASS	XXXXXXXX
Fecha	06/08/2019
ID	091052789

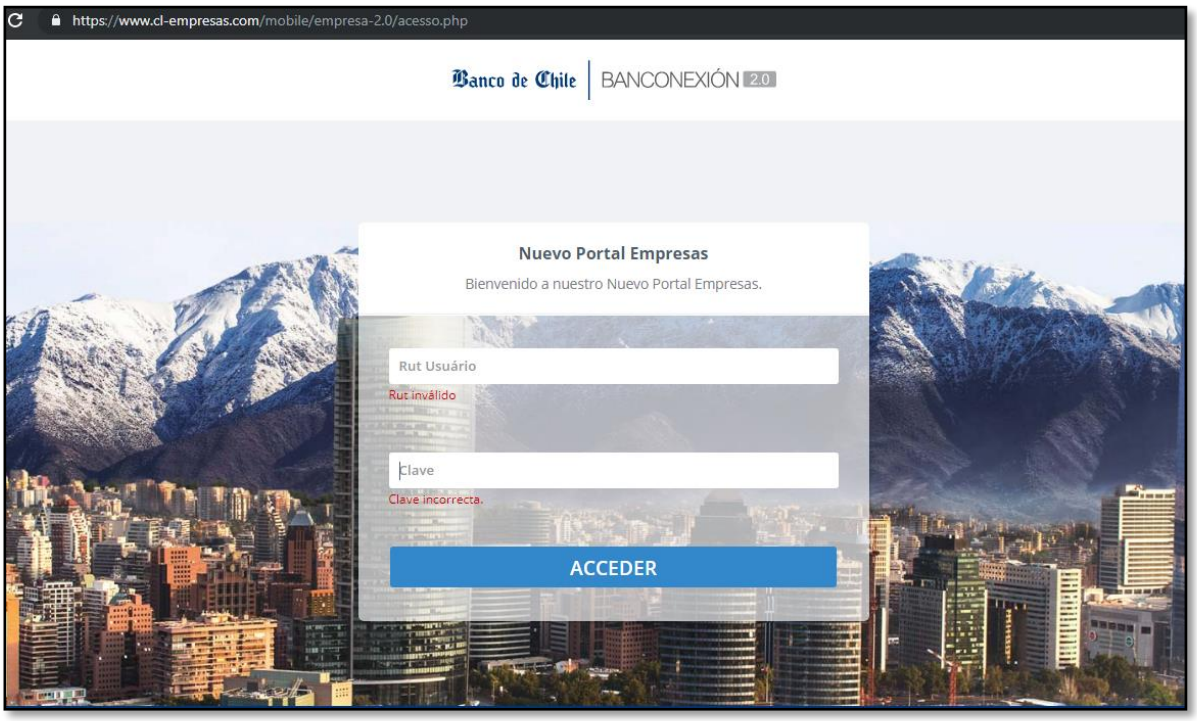
Banco de Chile

Informese sobre la garantia estatal de los depositos en su banco o en www.sbif.cl Ã‚Â© 2019 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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.08.06 15:11:07 -04'00'