

Alerta de seguridad informática	8FPH-00055-001
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Agosto de 2019
Última revisión	14 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 afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC 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 loC 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), ha identificado una campaña de phishing a través de un correo electrónico que intenta persuadir a los usuarios del Banco de Chile, para 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.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Url's:

[http://www\[.\]ahlam\[.\]pl](http://www[.]ahlam[.]pl)

[https://www\[.\]bancochile-cl\[.\]com/wps/26jzozngxp/dp199_persona/login_i9i1/index/loginqkiy/](https://www[.]bancochile-cl[.]com/wps/26jzozngxp/dp199_persona/login_i9i1/index/loginqkiy/)

Smtip Host

[95.217.10.55]

[37.233.92.98]

[37.233.92.164]

[37.233.92.165]

[37.233.92.194]

[37.233.92.145]

[37.233.93.26]

From:

root@37-233-92-98.planeetta[.]com

root@37-233-92-164.planeetta[.]com

root@37-233-92-165.planeetta[.]com

root@37-233-92-194.planeetta[.]com


root@37-233-92-145.planeetta[.]com


root@37-233-93-26.planeetta[.]com

Subject:

Banco de Chile - Verifica su Digipass. ID:

Imagen Phishing Correo

 bancochile@bancochile.cl |
[MENSAJE SOSPECHOSO] Banco de Chile - Verifica su Digipass. ID: 20192330101




Estimado(a)

Informamos que debes sincronizar su dispositivo Digipass, la sincronización corregirá los errores de código generados por su dispositivo.

La sincronización es obligatoria y debe realizarse hasta el 14/08/2019, de lo contrario, su cuenta será bloqueada por razones de seguridad.

Acceda a la opción abajo para sincronizar su Digipass.



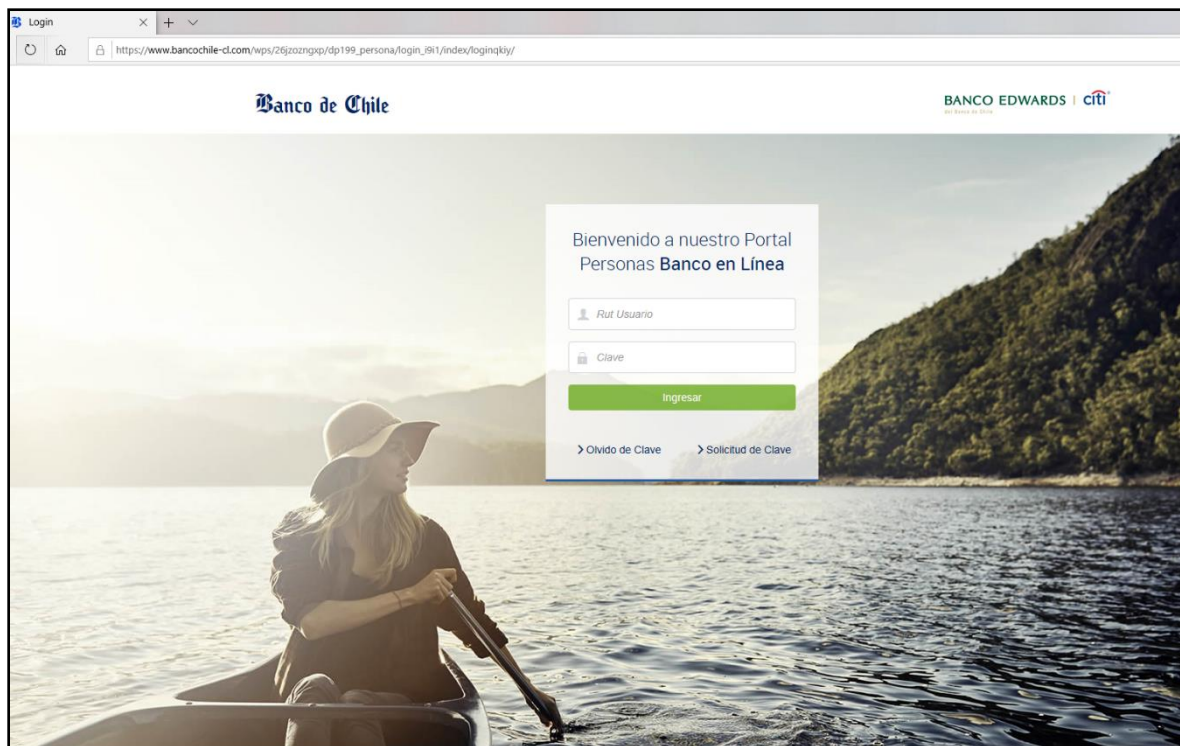
Datos de protocolo

Mail	
DIGIPASS	XXXXXXXX
Fecha	06/08/2019
ID	091052789

Banco de Chile

Informese sobre la garantía estatal de los depósitos en su banco o en www.sbif.cl © 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