Alerta de seguridad informática	**8FFR-00019-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**15 de Agosto de 2019**
Última revisión	**15 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 fraude no involucran a directamente a las entidades ni al sistema bancario, sino que son técnica de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, 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 llamado a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de un portal fraudulento que suplanta el sitio web oficial del **bancochile.cl** el que podría servir para robar credenciales de usuarios de esa entidad.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad bancaria aludida.

Indicadores de Compromisos

URL´s
https://www.bancochile-cl[.]com/wps/26jzozngxp/dp199_persona/login_i9i1/index/loginqkiy/

IP
104.28.24.106

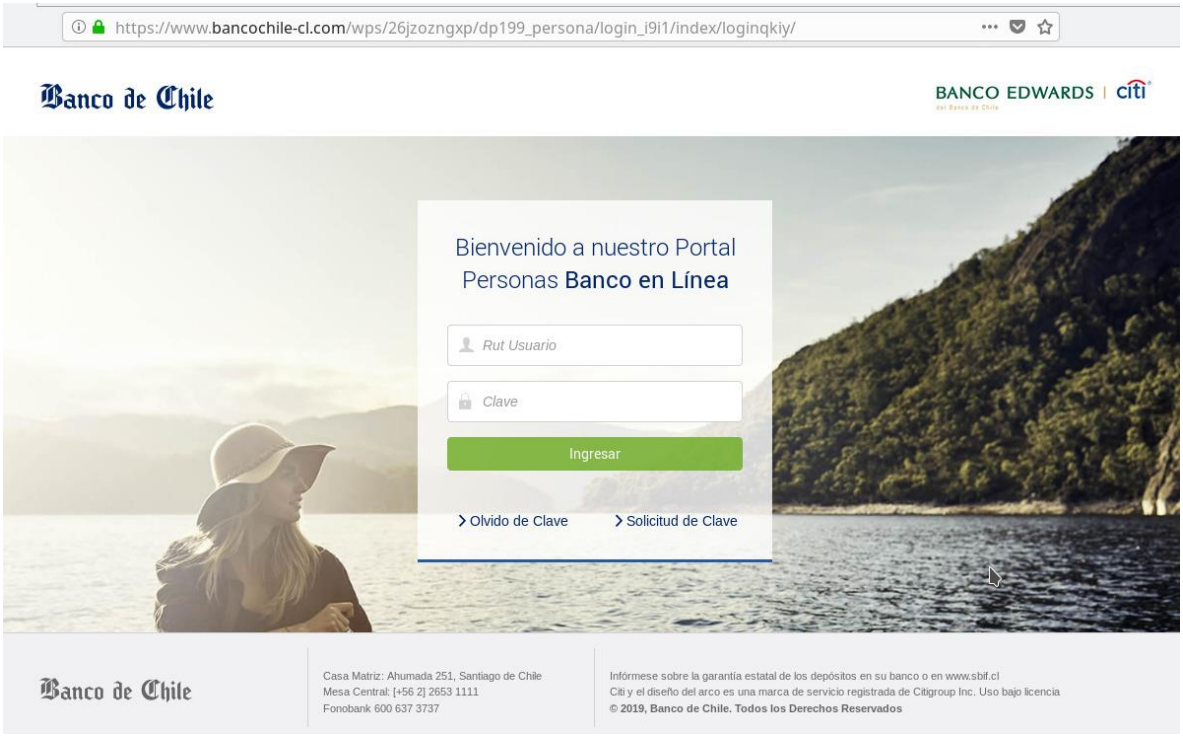
Localización
California Estados Unidos

Whois

Whois bancochile-cl.com

```
Domain Name: BANCOCHILE-CL.COM
Registrar WHOIS Server: whois.101domain.com
Registrar URL: https://www.101domain.com/
Updated Date: 2019-08-14T19:54:59Z
Creation Date: 2019-08-13T23:04:27Z
Registrar Registration Expiration Date: 2020-08-13T23:04:27Z
Registrar: https://www.101domain.com/
Registrar IANA ID: 1011
Registrar Abuse Contact Email: abuse@101domain.com
Registrar Abuse Contact Phone: +1.7604448674
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registrant Name: Private Registrant
Registrant Organization: Digital Privacy Corporation
Registrant Street:  3220 Executive Ridge Drive, Suite 101.
Registrant Street: C/O BANCOCHILE-CL.COM
Registrant City: Vista
Registrant State/Province: CA
Registrant Postal Code: 92081
Registrant Country: US
Registrant Phone: +1.7604482392
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 22be8e.RidW7pmqtYN@digitalprivacy.co
Admin Name: Private Registrant
Admin Organization: Digital Privacy Corporation
Admin Street:  3220 Executive Ridge Drive, Suite 101.
Admin Street: C/O BANCOCHILE-CL.COM
Admin City: Vista
Admin State/Province: CA
Admin Postal Code: 92081
Admin Country: US
Admin Phone: +1.7604482392

Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 22be8e.RidW7pmqtYN@digitalprivacy.co
Name Server: NORMAN.NS.CLOUDFLARE.COM
Name Server: CANDY.NS.CLOUDFLARE.COM
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net
For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
>>> Last update of WHOIS database: 2019-08-14T20:52:11Z <<<


If you believe this domain is in violation of our terms and conditions,
please complete an abuse complaint at

 https://www.101domain.com/report_abuse.htm

and our team will investigate accordingly.
```

Ejemplo de Imagen del sitio



Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido
- 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

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.08.15
10:23:13 -04'00'