Alerta de seguridad informática	**8FFR-00057-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**13 de Septiembre de 2019**
Última revisión	**13 de Septiembre 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 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 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 llamados 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 asociado a una IP que suplanta el sitio web oficial del **banco Chile,** 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.

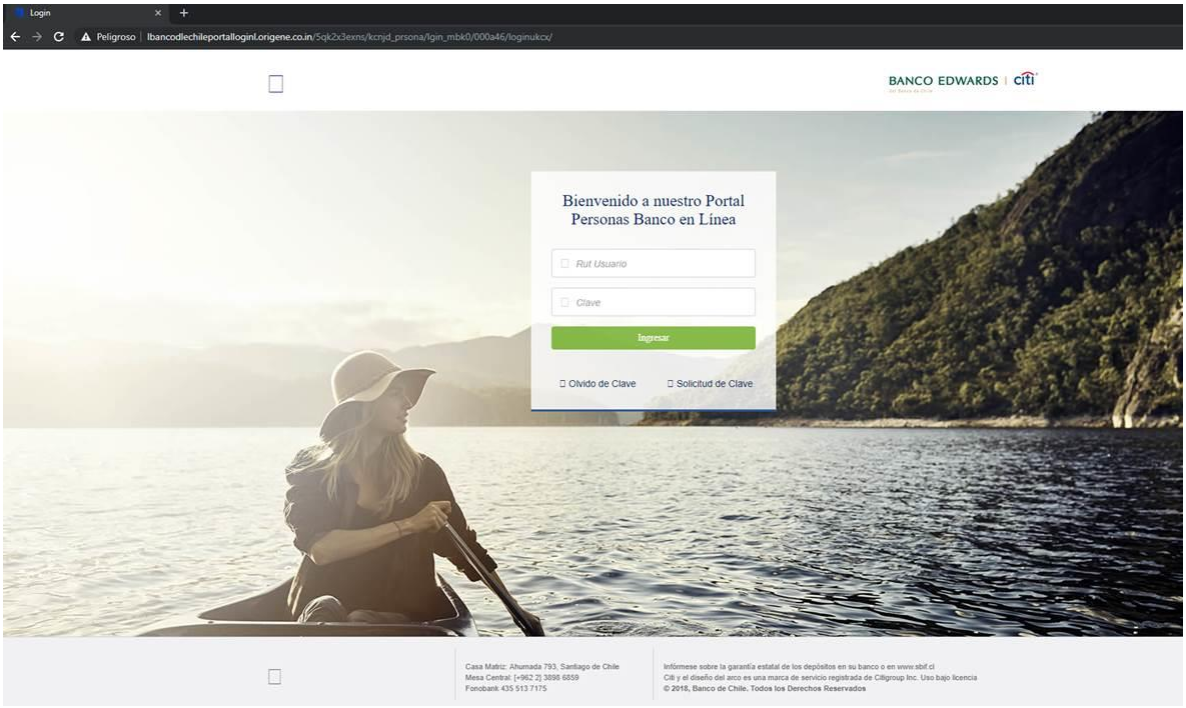
Indicadores de Compromisos

URL de redirección:
https:[//]www[.]lbancodlechileportalloginl[.]origene[.]co[.]in/5qk2x3exns/kcnjd_prsona/lgin_mbk0/000a46/loginukcx/

IP´s
66[.]7[.]148[.]252

Localización
Conshohocken, Pennsylvania, Estados Unidos

Ejemplo de Imagen del sitio



Whois

```
soc@kali:~$ whois co.in
Domain Name: co.in
Registry Domain ID: D5499738-IN
Registrar WHOIS Server:
Registrar URL:
Updated Date: 2019-02-24T14:25:25Z
Creation Date: 2011-11-14T19:49:37Z
Registry Expiry Date: 2021-11-14T19:49:37Z
Registrar: Neustar 1
Registrar IANA ID: 700000
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferP
rohibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhi
bited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhi
bited
Registry Registrant ID:
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: Delhi
Registrant Postal Code:
Registrant Country: IN
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Please contact the Registrar listed above
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin Street:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Please contact the Registrar listed above
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech Street:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
```

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, hacia la URL maliciosa
- 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: 2019.09.13
16:55:12 -03'00'