Alerta de seguridad informática	8FFR20-00254-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Marzo de 2020
Última revisión	11 de Marzo de 2020

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 BCI, 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

bcipersonaslogin[.]c

Domain bcipersonaslogin.cl

bcipersonaslogin / cl / Subdomains

record type	TTL	value		
A	14400	162.241.60.80		
NS	86400	nspro11.hostgator.cl	Zones on DNS server	162.241.60.78
NS	86400	nspro10.hostgator.cl	Zones on DNS server	162.241.60.77
MX	14400	0 mail.bcipersonaslogin.cl		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname: nspro10.hostgator.cl Rname: root.sh-pro10.hostgator.cl Serial number: 2020030904 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

Ilustración 1 Dominio donde se Aloja Url del Banco BCI Falso y DNS que utiliza

Certificados

Subject DN CN=bcipersonaslogin.cl

Issuer DN C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA

Serial 235448627913599711454273318866827450287

Validity 2020-03-09 00:00:00 **to** 2021-03-09 23:59:59 (365 days, 23:59:59)

Names bcipersonaslogin.cl
www.bcipersonaslogin.cl

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco BCI

IP
162[.]241[.]60[.]80

Domain bcipersonaslogin.cl is located on IP address << 162.241.60.80 >>	
Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	46606
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco BCI

Localización
Provo, Utah, Estados Unidos

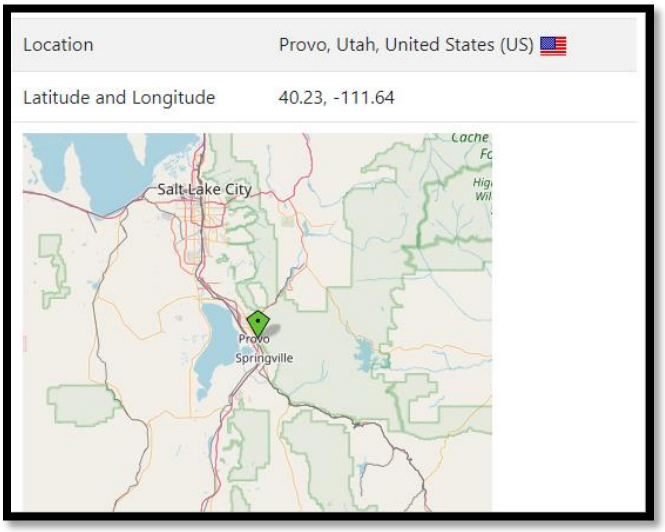
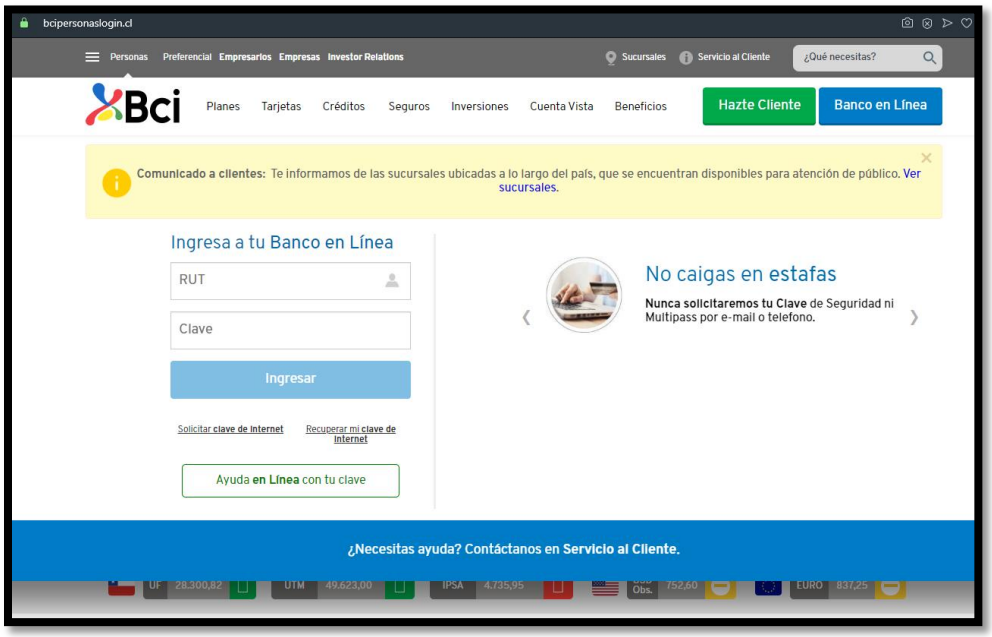


Imagen del sitio



Whois

```
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: bcipersonaslogin.cl
Registrant name: jose perez
Registrant organisation: N/A
Registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar URL: https://www.publicdomainregistry.com
Creation date: 2020-03-09 09:16:21 CLST
Expiration date: 2021-03-09 09:16:21 CLST
Name server: nsprol0.hostgator.cl
Name server: nsproll.hostgator.cl

%%
%% For communication with domain contacts please use website.
%% See https://www.nic.cl/registry/Whois.do?d=bcipersonaslogin.cl
%%
```

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: 2020.03.11 12:00:42 -03'00'