Alerta de seguridad informática	8FFR20-00205-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de Febrero de 2020
Última revisión	04 de Febrero 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 de **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

URLs

bci[.]cl[.]acceso-cl[.]in/inicio

Domain acceso-cl.in

acceso-cl / in / Subdomains

record type	TTL	value		
NS	36000	2-can.njalla.in	Zones on DNS server	185.193.124.34
NS	36000	3-get.njalla.fo	Zones on DNS server	95.215.19.5
NS	36000	1-you.njalla.no	Zones on DNS server	185.193.124.2
SOA	10800	Mname	1-you.njalla.no	
		Rname	you.can-get-no.info	
		Serial number	2001311622	
		Refresh	21600	
		Retry	7200	
		Expire	1814400	
		Minimum TTL	86400	

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

Certificados

Subject DN	CN=bci.cl.acceso-cl.in
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	277048761003857979794336490695799635062913
Validity	2020-01-31 15:25:45 **to** 2020-04-30 15:25:45 (90 days, 0:00:00)
Names	bci.cl.acceso-cl.in

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

IPs

142[.]93[.]226[.]63

Domain bci.cl.acceso-cl.in is located on IP address << 142.93.226.63 >>

Block start	142.93.0.0
End of block	142.93.255.255
Block size	65536 Domains in block
Block name	SEARSCANADA-93
AS number	14061
Parent block	142.0.0.0 - 142.255.255.255
Organization	Sears Canada Inc.
City	NORTH YORK
Region/State	Ontario
Country	CA , Canada
Reg. date	1991-12-30
Host name	no record in reverse zone
Domain count	>= 3 Servers around
Domains	1 bci.cl.acceso-cl.in 2 scotia.cl.acceso-cl.com 3 scotia.cl.acceso-cl.in

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

Localización

Netherlands, Amsterdam, Noord-Holland

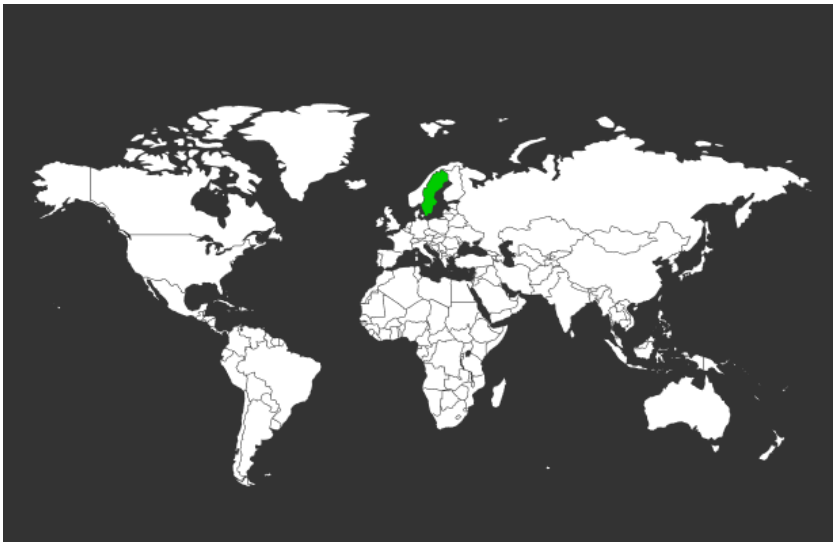
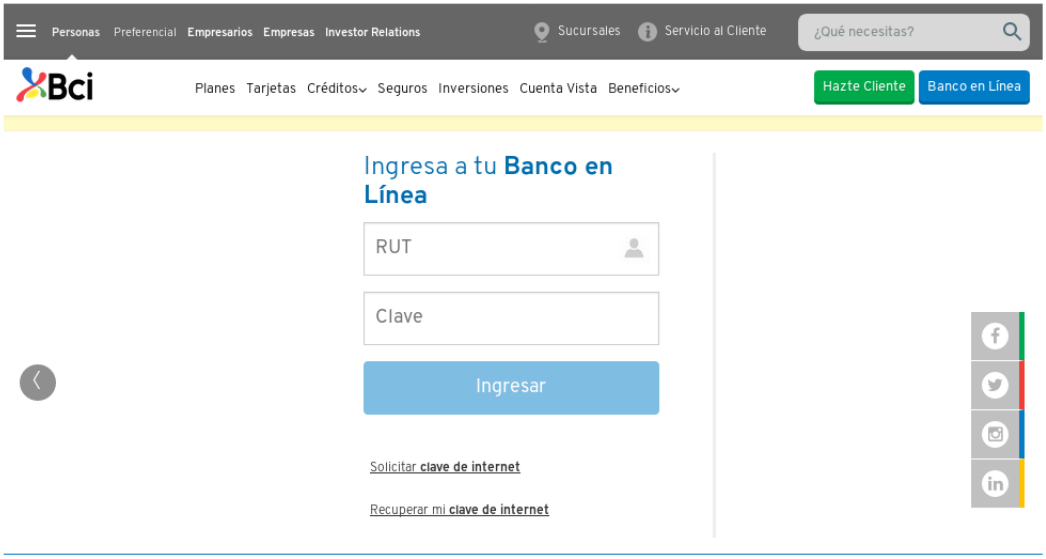


Imagen del sitio



Whois

```
Domain Name: acceso-cl.in
Registry Domain ID: D7EF97451A9644B3692C09D118E1E4CF8-IN
Registrar WHOIS Server:
Registrar URL: http://www.opensrs.com
Updated Date: 2020-01-22T23:52:51Z
Creation Date: 2020-01-17T23:52:51Z
Registry Expiry Date: 2021-01-17T23:52:51Z
Registrar: Tucows Inc.
Registrar IANA ID: 69
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferP
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhi
Registry Registrant ID:
Registrant Name:
Registrant Organization: Data Protected
Registrant Street:
Registrant Street:
Registrant Street:
Registrant City:
Registrant State/Province: ON
Registrant Postal Code:
Registrant Country: CA
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:
Tech Fax:
Tech Fax Ext:
Tech Email: Please contact the Registrar listed above
Name Server: 2-can.njalla.in
Name Server: 3-get.njalla.fo
Name Server: 1-you.njalla.no
DNSSEC: unsigned
```

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: 2020.02.04 15:43:17 -03'00'