Alerta de seguridad cibernética	8FFR20-00296-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 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 portale 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 COMPROMISO

URL
acceso-bci[.]cl

IP
162[.]241[.]61[.]53

DOMINIOS DONDE SE ALOJA URL

Domain acceso-bci.cl

acceso-bci / cl / Subdomains

record type	TTL	value		
A	14400	162.241.61.53		
NS	86400	nspro12.hostgator.cl	Zones on DNS server	162.241.61.51
NS	86400	nspro13.hostgator.cl	Zones on DNS server	162.241.61.52
MX	14400	0 mail.acceso-bci.cl		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname: nspro12.hostgator.cl Rname: root.sh-pro12.hostgator.cl Serial number: 2020032904 Refresh: 86400 Retry: 7200 Expire: 3600000 Minimum TTL: 86400		

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2642257308	2020-03-29	2020-03-29	2021-03-29	acceso-bci.cl www.acceso-bci.cl	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
2642257309	2020-03-29	2020-03-29	2021-03-29	acceso-bci.cl www.acceso-bci.cl	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain acceso-bci.cl is located on IP address << 162.241.61.53 >>	
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

LOCALIZACIÓN

Provo, Utah, Estados Unidos

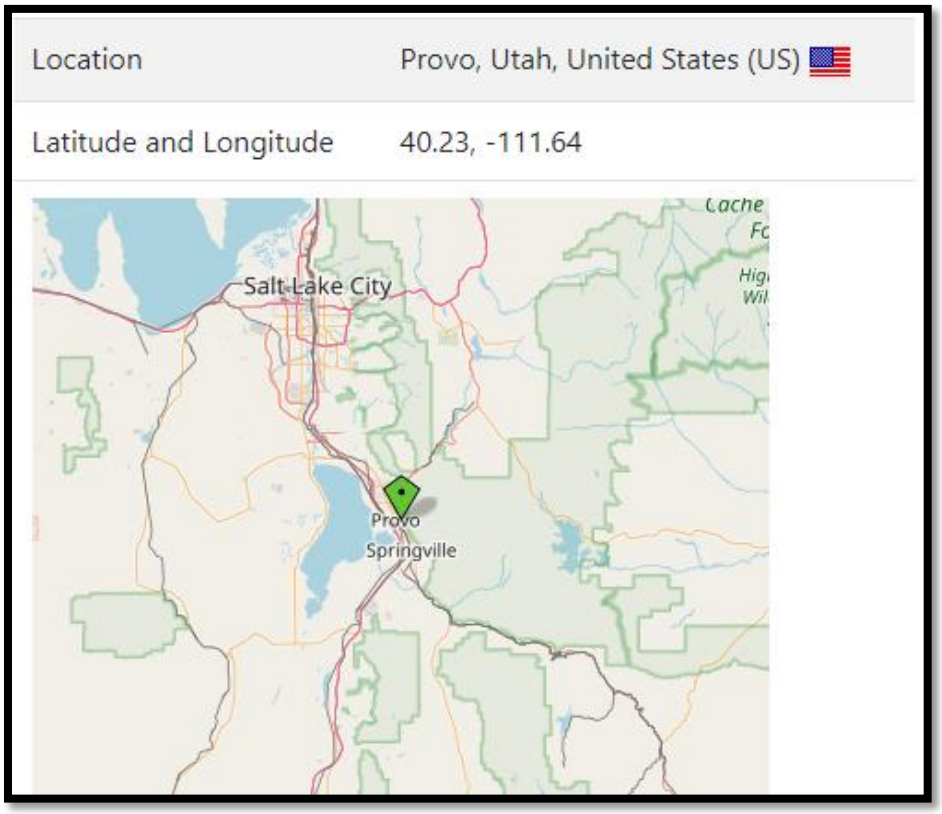
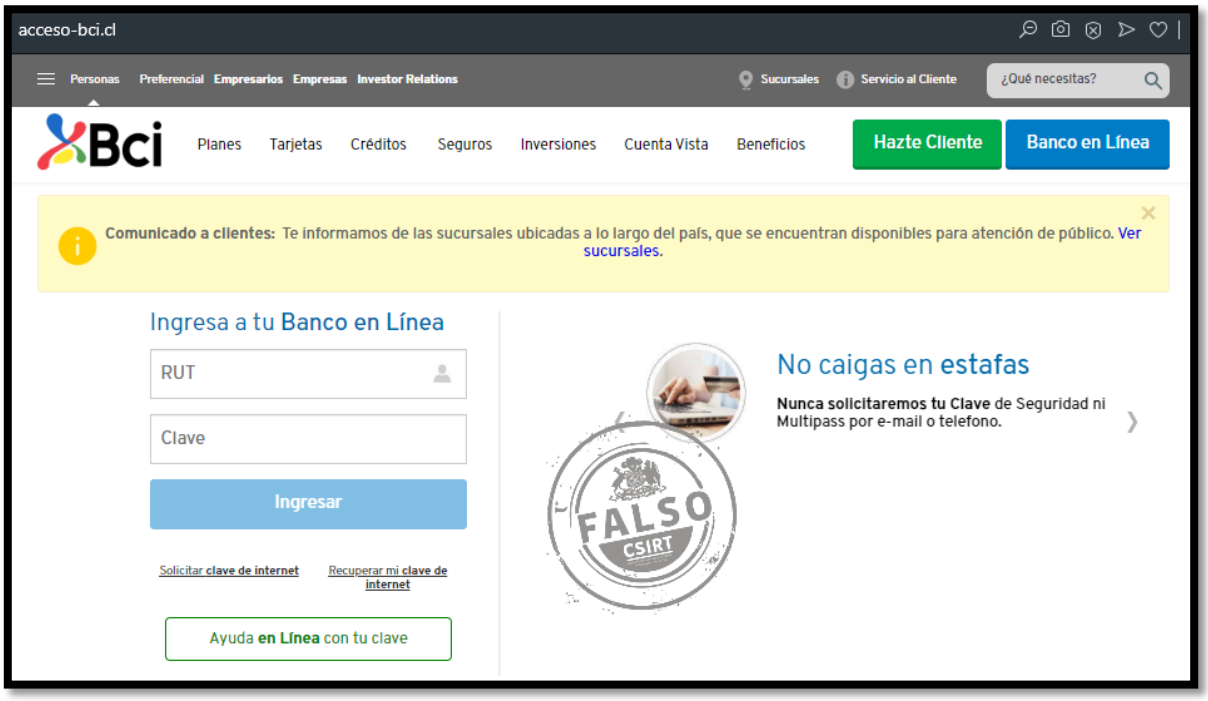


IMAGEN DEL SITIO



WHOIS

```
Domain name: acceso-bci.cl
Registrant name: manuel perez
Registrant organisation: N/A
Registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar URL: https://www.publicdomainregistry.com
Creation date: 2020-03-29 13:22:15 CLST
Expiration date: 2021-03-29 13:22:15 CLST
Name server: nspro12.hostgator.cl
Name server: nspro13.hostgator.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.