| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00299-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 01 de abril de 2020 |
| Última revisión | 01 de abril 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 detectado la activación de dos portales fraudulentos asociados a dos IPs que suplantan 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

URLs
bci-informa[.]cl
bci-accesos[.]cl

IPs
162[.]241[.]61[.]53
162[.]241[.]2[.]177

# DOMINIOS DONDE SE ALOJAN URLs

**Domain bci-accesos.cl**

bci-accesos / cl / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 14400 | 162.241.2.177 | | |
| NS | 86400 | ns12.hostgator.cl | Zones on DNS server | 162.241.2.174 |
| NS | 86400 | ns13.hostgator.cl | Zones on DNS server | 162.241.2.175 |
| MX | 14400 | 0 mail.bci-accesos.cl | | |
| TXT | 14400 | v=spf1 a mx include:websitewelcome.com ~all | | |
| SOA | 86400 | Mname | ns12.hostgator.cl | |
| | | Rname | root.shared12.hostgator.cl | |
| | | Serial number | 2020033102 | |
| | | Refresh | 86400 | |
| | | Retry | 7200 | |
| | | Expire | 3600000 | |
| | | Minimum TTL | 86400 | |

**Domain bci-informa.cl**

bci-informa / 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.bci-informa.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 | 2020040104 | |
| | | Refresh | 86400 | |
| | | Retry | 7200 | |
| | | Expire | 3600000 | |
| | | Minimum TTL | 86400 | |

# CERTIFICADOS

## Certificate Name matches bci-informa.cl


Subject bci-informa.cl

Valid from 01/Apr/2020 to 01/Apr/2021

Issuer Sectigo RSA Domain Validation Secure Server CA

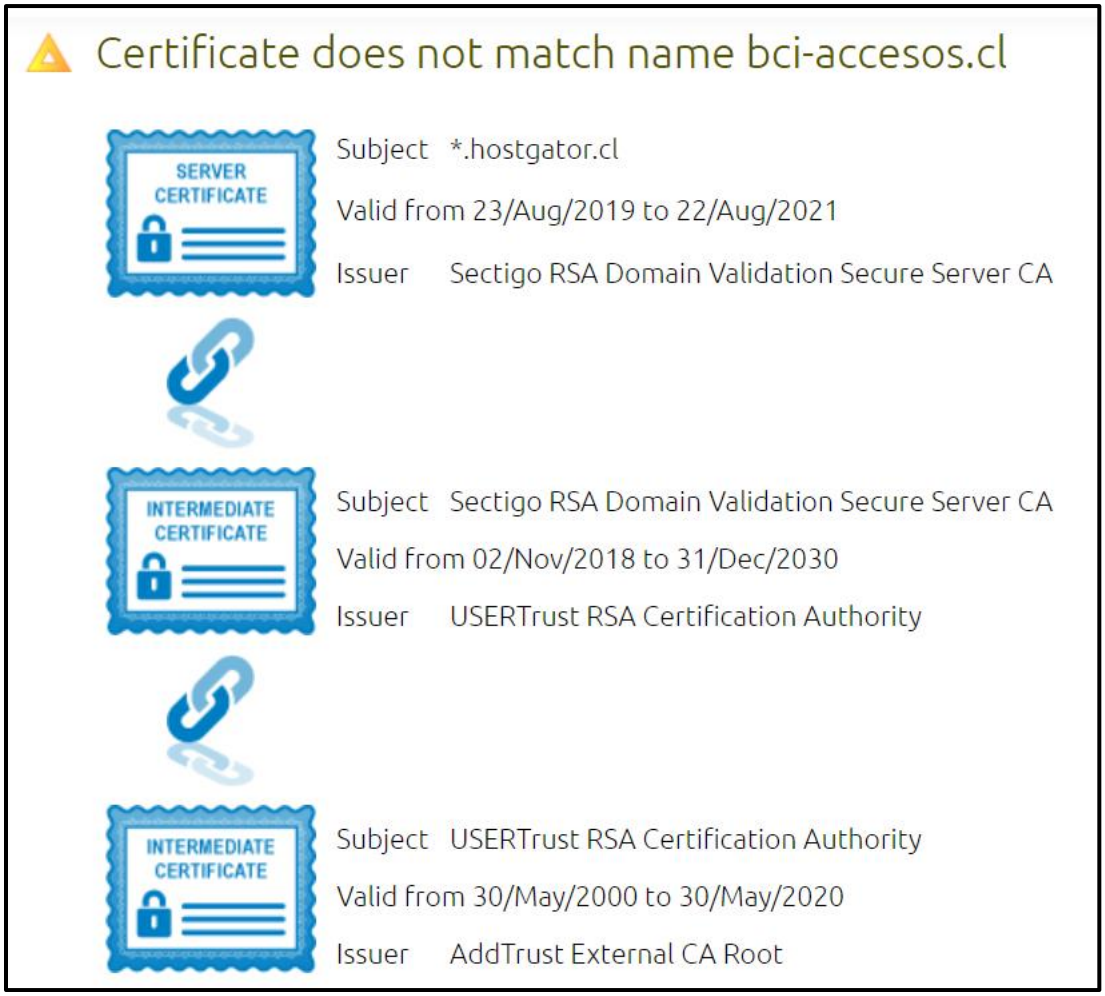

Subject Sectigo RSA Domain Validation Secure Server CA

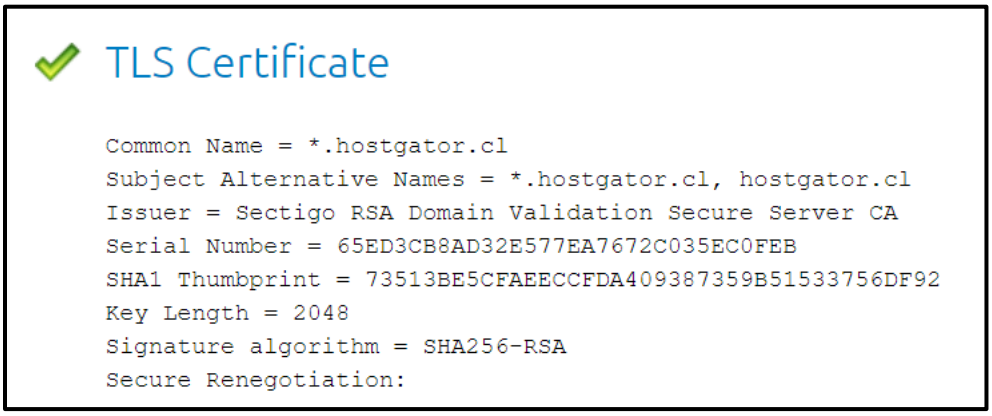
Valid from 02/Nov/2018 to 31/Dec/2030

Issuer USERTrust RSA Certification Authority

## TLS Certificate

```
Common Name = bci-informa.cl
Subject Alternative Names = bci-informa.cl, www.bci-informa.cl
Issuer = Sectigo RSA Domain Validation Secure Server CA
Serial Number = 860A0E3D38DA0631059B0BE59414F602
SHA1 Thumbprint = D1FE100CD79FF764FCF0A35A7EEFB94D1C9F019C
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```


Certificate does not match name bci-accesos.cl
SERVER CERTIFICATE
Subject *.hostgator.cl
Valid from 23/Aug/2019 to 22/Aug/2021
Issuer Sectigo RSA Domain Validation Secure Server CA
INTERMEDIATE CERTIFICATE
Subject Sectigo RSA Domain Validation Secure Server CA
Valid from 02/Nov/2018 to 31/Dec/2030
Issuer USERTrust RSA Certification Authority
INTERMEDIATE CERTIFICATE
Subject USERTrust RSA Certification Authority
Valid from 30/May/2000 to 30/May/2020
Issuer AddTrust External CA Root


TLS Certificate
Common Name = *.hostgator.cl
Subject Alternative Names = *.hostgator.cl, hostgator.cl
Issuer = Sectigo RSA Domain Validation Secure Server CA
Serial Number = 65ED3CB8AD32E577EA7672C035EC0FEB
SHA1 Thumbprint = 73513BE5CFAEECCFDA409387359B51533756DF92
Key Length = 2048
Signature algorithm = SHA256-RSA
Secure Renegotiation:

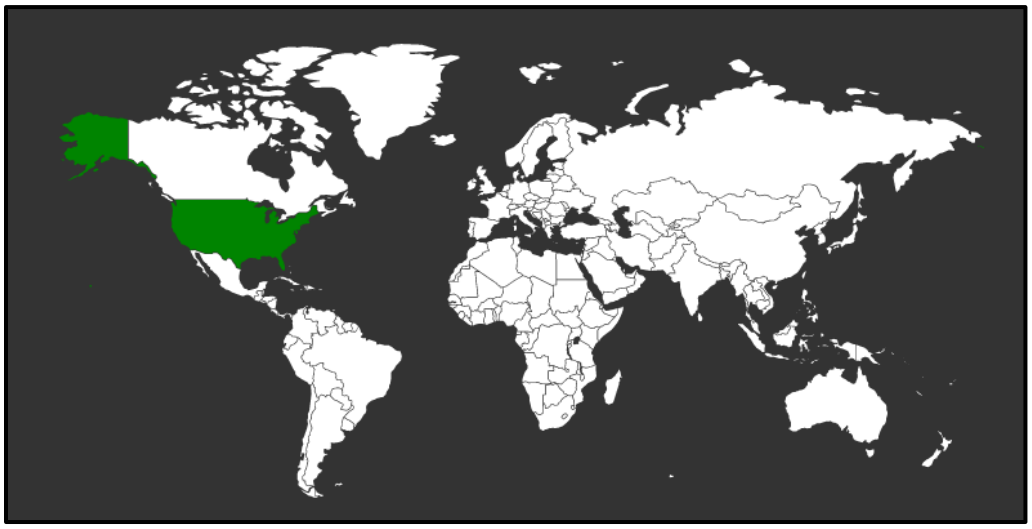
# IPs DE ORIGEN DONDE SE ALOJA SITIO

| Domain bci-informa.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 |

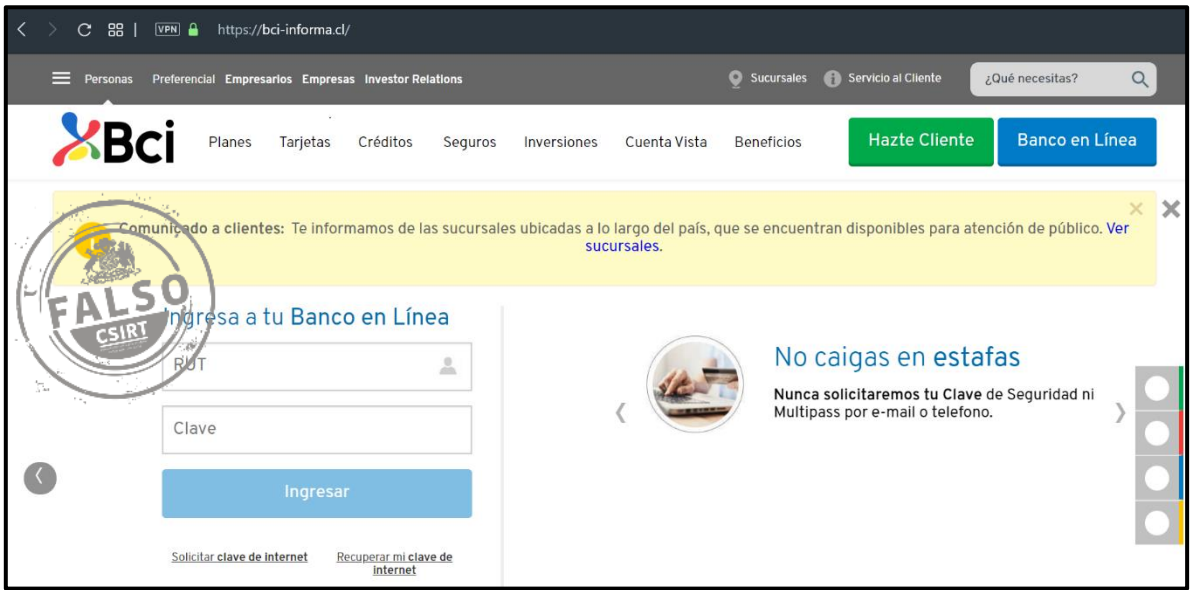
| Domain bci-accesos.cl is located on IP address << 162.241.2.177 >> | |
|---|---|
| **Block start** | 162.240.0.0 |
| **End of block** | 162.241.255.255 |
| **Block size** | 131072 Domains in block |
| **Block name** | UNIFIEDLAYER-NETWORK-16 |
| **AS number** | 46606 |
| **Parent block** | 162.0.0.0 - 162.255.255.255 |
| **Organization** | UnifiedLayer |

# LOCALIZACIÓN

Provo, Utah, Estados Unidos



# IMAGEN DEL SITIO




## WHOIS

```
Domain name: bci-accesos.cl
Registrant name: Hernan Hernahansen vik torres
Registrant organisation: N/A
Registrar name: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar URL: https://www.publicdomainregistry.com
Creation date: 2020-04-01 07:51:54 CLST
Expiration date: 2021-04-01 07:51:54 CLST
Name server: ns12.hostgator.cl
Name server: ns13.hostgator.cl
```

```
Domain name: bci-informa.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: 2020-03-31 21:02:33 CLST
Expiration date: 2021-03-31 21:02:33 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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.01 13:58:08 -03'00'