Alerta de seguridad informática	8FFR-00125-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Noviembre de 2019
Última revisión	24 de Noviembre 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 tres portales fraudulentos asociados a tres IPs que suplantan el sitio web oficial de **Banco de 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´s

URL Sitio Clonado:
https[://]qrcoach[.]com/wp-admin/js/servicio/nuevo/www[.]bancochile[.]cl
www[.]gigalan[.]pe/wp-content/uploads/2018/06/servicios/

Domain qrcoach.com

qrcoach / com / Subdomains

record type	TTL	value		
A	300	104.27.177.193		
A	300	104.27.176.193		
NS	86400	jean.ns.cloudflare.com	Zones on DNS server	173.245.58.121
NS	86400	tim.ns.cloudflare.com	Zones on DNS server	173.245.59.145
TXT	300	ca3-7454c7acce0e486aa25352bef76c9a5f		
SOA	3600	Mname: jean.ns.cloudflare.com Rname: dns.cloudflare.com Serial number: 2031888129 Refresh: 10000 Retry: 2400 Expire: 604800 Minimum TTL: 3600		

Domain qrcoach.com

qrcoach / com / Subdomains

record type	TTL	value		
A	300	104.27.177.193		
A	300	104.27.176.193		
NS	86400	jean.ns.cloudflare.com	Zones on DNS server	173.245.58.121
NS	86400	tim.ns.cloudflare.com	Zones on DNS server	173.245.59.145
TXT	300	ca3-7454c7acce0e486aa25352bef76c9a5f		
SOA	3600	Mname: jean.ns.cloudflare.com Rname: dns.cloudflare.com Serial number: 2031888129 Refresh: 10000 Retry: 2400 Expire: 604800 Minimum TTL: 3600		

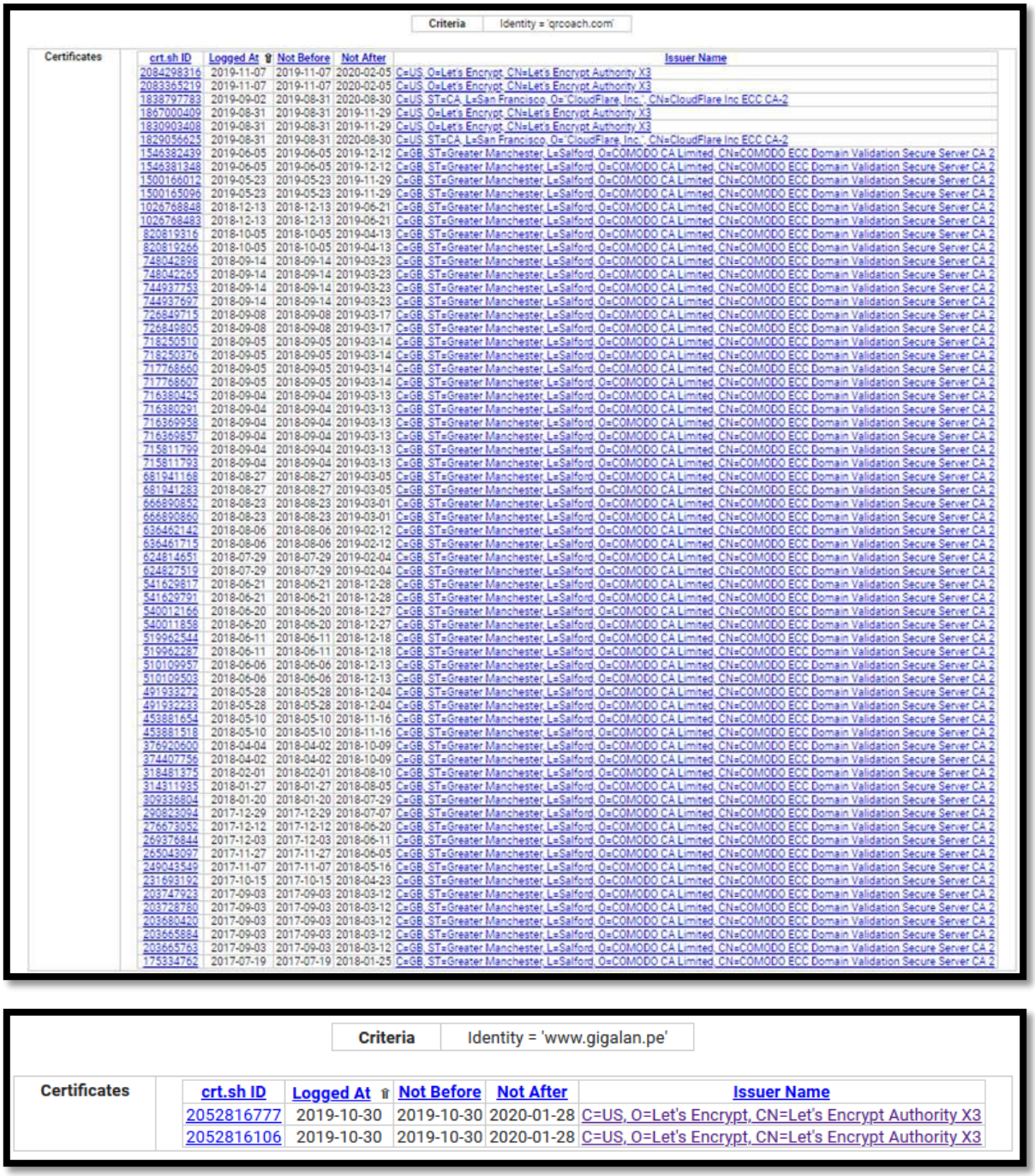
Domain www.gigalan.pe

www / gigalan / pe / Subdomains

record type	TTL	value	
CNAME	38400	www.gigalan.com.pe	181.224.229.10

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

Certificados



Criteria: Identity = 'qrcoach.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2084298316	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2083365219	2019-11-07	2019-11-07	2020-02-05	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1838797783	2019-09-02	2019-08-31	2020-08-30	C=US, ST=CA, L=San Francisco, O="CloudFlare, Inc.", CN=CloudFlare Inc ECC CA-2
1867000409	2019-08-31	2019-08-31	2019-11-29	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1830903408	2019-08-31	2019-08-31	2019-11-29	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1829056625	2019-08-31	2019-08-31	2020-08-30	C=US, ST=CA, L=San Francisco, O="CloudFlare, Inc.", CN=CloudFlare Inc ECC CA-2
1546382439	2019-06-05	2019-06-05	2019-12-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1546381348	2019-06-05	2019-06-05	2019-12-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1500166012	2019-05-23	2019-05-23	2019-11-29	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1500165096	2019-05-23	2019-05-23	2019-11-29	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1026768848	2018-12-13	2018-12-13	2019-06-21	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
1026768483	2018-12-13	2018-12-13	2019-06-21	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
820819316	2018-10-05	2018-10-05	2019-04-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
820819266	2018-10-05	2018-10-05	2019-04-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
748042898	2018-09-14	2018-09-14	2019-03-23	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
748042265	2018-09-14	2018-09-14	2019-03-23	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
744937753	2018-09-14	2018-09-14	2019-03-23	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
744937697	2018-09-14	2018-09-14	2019-03-23	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
726849715	2018-09-08	2018-09-08	2019-03-17	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
726849805	2018-09-08	2018-09-08	2019-03-17	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
718250510	2018-09-05	2018-09-05	2019-03-14	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
718250376	2018-09-05	2018-09-05	2019-03-14	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
717768660	2018-09-05	2018-09-05	2019-03-14	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
717768607	2018-09-05	2018-09-05	2019-03-14	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
716380425	2018-09-04	2018-09-04	2019-03-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
716380291	2018-09-04	2018-09-04	2019-03-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
716369958	2018-09-04	2018-09-04	2019-03-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
716369857	2018-09-04	2018-09-04	2019-03-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
715811799	2018-09-04	2018-09-04	2019-03-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
715811793	2018-09-04	2018-09-04	2019-03-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
681941168	2018-08-27	2018-08-27	2019-03-05	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
681941283	2018-08-27	2018-08-27	2019-03-05	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
666890852	2018-08-23	2018-08-23	2019-03-01	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
666890860	2018-08-23	2018-08-23	2019-03-01	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
636462142	2018-08-06	2018-08-06	2019-02-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
636461715	2018-08-06	2018-08-06	2019-02-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
624814651	2018-07-29	2018-07-29	2019-02-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
624827519	2018-07-29	2018-07-29	2019-02-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
541629817	2018-06-21	2018-06-21	2018-12-28	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
541629791	2018-06-21	2018-06-21	2018-12-28	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
540012166	2018-06-20	2018-06-20	2018-12-27	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
540011858	2018-06-20	2018-06-20	2018-12-27	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
519962544	2018-06-11	2018-06-11	2018-12-18	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
519962287	2018-06-11	2018-06-11	2018-12-18	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
510109957	2018-06-06	2018-06-06	2018-12-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
510109503	2018-06-06	2018-06-06	2018-12-13	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
491933272	2018-05-28	2018-05-28	2018-12-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
491932233	2018-05-28	2018-05-28	2018-12-04	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
453881654	2018-05-10	2018-05-10	2018-11-16	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
453881518	2018-05-10	2018-05-10	2018-11-16	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
376920600	2018-04-04	2018-04-02	2018-10-09	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
374407756	2018-04-02	2018-04-02	2018-10-09	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
318481375	2018-02-01	2018-02-01	2018-08-10	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
314311935	2018-01-27	2018-01-27	2018-08-05	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
309336804	2018-01-20	2018-01-20	2018-07-29	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
290823094	2017-12-29	2017-12-29	2018-07-07	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
276673052	2017-12-12	2017-12-12	2018-06-20	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
269376844	2017-12-03	2017-12-03	2018-06-11	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
265043097	2017-11-27	2017-11-27	2018-06-05	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
249043549	2017-11-07	2017-11-07	2018-05-16	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
231693192	2017-10-15	2017-10-15	2018-04-23	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
203747923	2017-09-03	2017-09-03	2018-03-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
203728780	2017-09-03	2017-09-03	2018-03-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
203680420	2017-09-03	2017-09-03	2018-03-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
203665884	2017-09-03	2017-09-03	2018-03-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
203665763	2017-09-03	2017-09-03	2018-03-12	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2
175334762	2017-07-19	2017-07-19	2018-01-25	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO ECC Domain Validation Secure Server CA 2

Criteria: Identity = 'www.gigalan.pe'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2052816777	2019-10-30	2019-10-30	2020-01-28	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2052816106	2019-10-30	2019-10-30	2020-01-28	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco de Chile

IP

104.27.176.193

104.27.177.193

181.224.229.10

Domain qrcoach.com is located on IP address << 104.27.176.193 >>	
Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 Domains in block
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.
City	San Francisco
Region/State	California
Country	US , United States
Reg. date	2014-03-28
Host name	no record
Web server	cloudflare-nginx

Domain qrcoach.com is located on IP address << 104.27.177.193 >>	
Block start	104.16.0.0
End of block	104.31.255.255
Block size	1048576 Domains in block
Block name	CLOUDFLARENET
AS number	13335
Parent block	104.0.0.0 - 104.255.255.255
Organization	CloudFlare, Inc.
City	San Francisco
Region/State	California
Country	US , United States
Reg. date	2014-03-28
Host name	no record
Web server	cloudflare-nginx

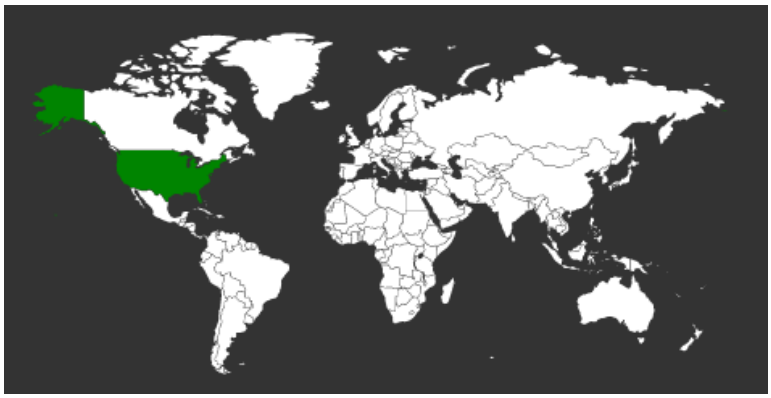
Domain www.gigalan.pe is located on IP address << 181.224.229.10 >>

Block start	181.224.224.0
End of block	181.224.255.255
Block size	8192 Domains in block
Block name	
AS number	262253
Parent block	181.0.0.0 - 181.255.255.255
Organization	ECONOCABLE MEDIA SAC
City	Lima
Region/State	Lima
Country	PE , Peru
Reg. date	2012-12-03
Host name	fhs01.flx.com.pe
Domains	1 www.gigalan.pe

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

Localización

Dallas, Texas, Estados Unidos



Lima, Lima, Perú

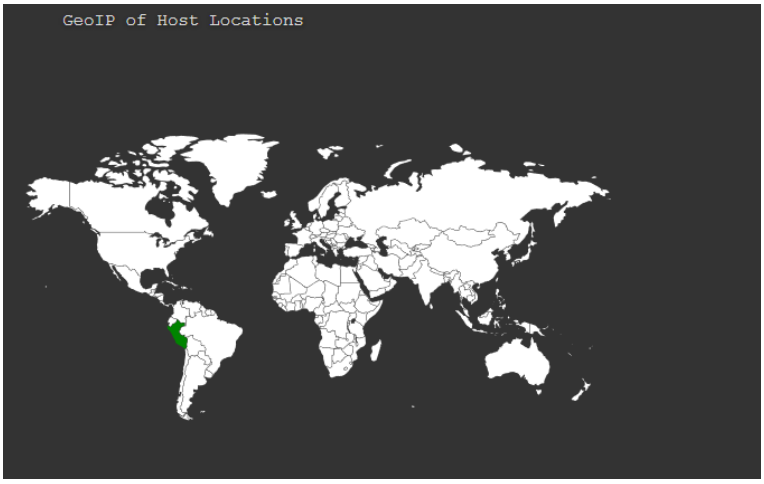
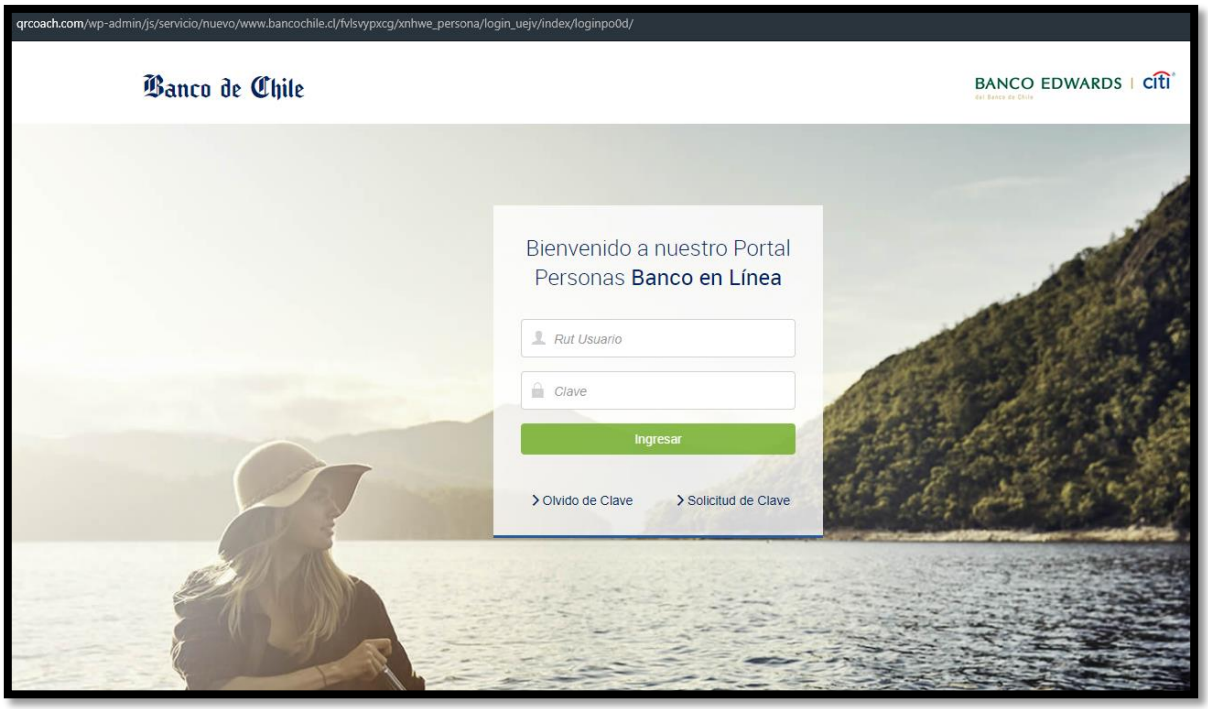
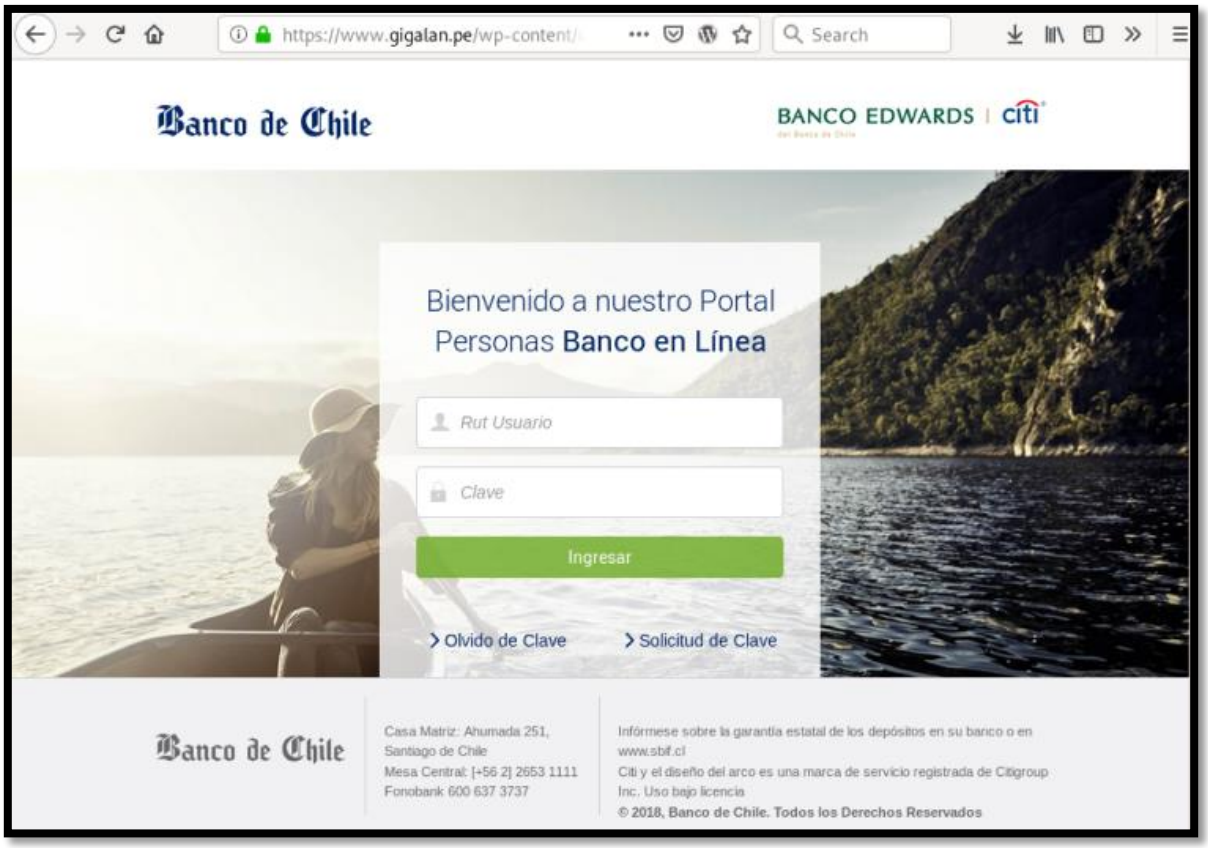


Imagen del sitio





Whois

```
Domain Name: qrcoach.com
Registry Domain ID: 2144656532_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-08-30T19:19:36Z
Creation Date: 2017-07-19T16:57:09Z
Registrar Registration Expiration Date: 2020-07-19T16:57:09Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization: Ocean's Bridge Group Ltd
Registrant State/Province: Oregon
Registrant Country: US
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=qrcoa
ch.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=qrcoach.co
m
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=qrcoach.com
Name Server: JEAN.NS.CLOUDFLARE.COM
Name Server: TIM.NS.CLOUDFLARE.COM
DNSSEC: unsigned
```

```
Domain Name: gigalan.pe
WHOIS Server: NIC .PE
Sponsoring Registrar: NIC .PE
Domain Status: ok
Registrant Name: fiberlux sac
Admin Name: fiberlux sac
Admin Email: ssalas@flx.com.pe
Name Server: ns1.fiberluxperu.com
Name Server: ns2.fiberluxperu.com
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: 2019.11.24 12:11:23 -03'00'