Alerta de seguridad informática	**8FFR-00066-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**23 de Septiembre de 2019**
Última revisión	**23 de Septiembre 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 dos portales fraudulentos asociados a IP's 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.

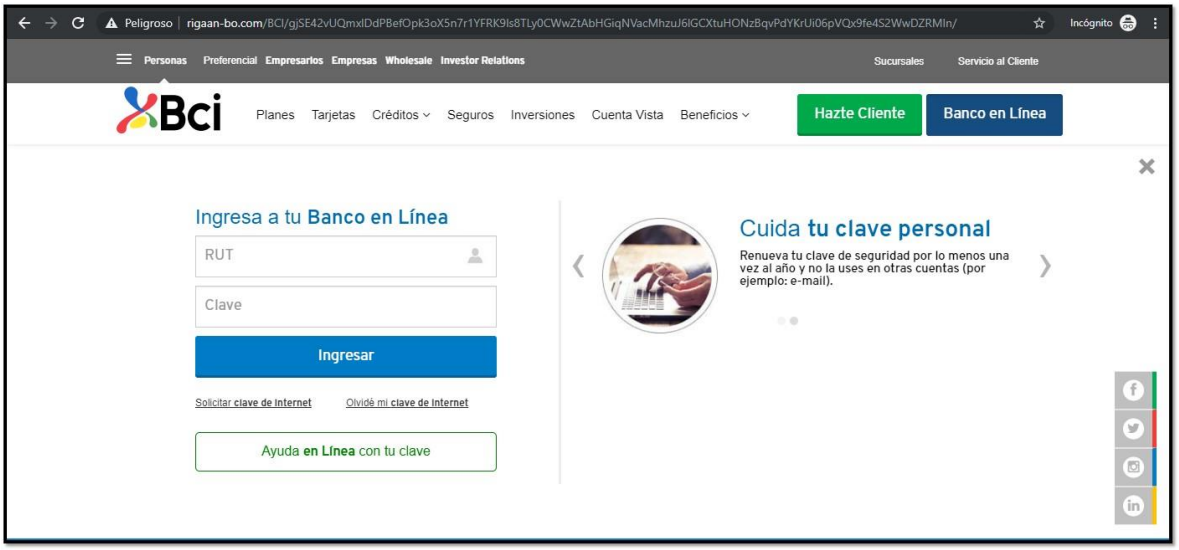
Indicadores de Compromisos

URL´s
https[://]www[.]bcipersonas[.]com/choose[.]php
https[://]rigaan-bo[.]com/BCl/gjSE42vUQmxlDdPBefOpk3oX5n7r1YFRK9Is8TLy0CWwZtAbHGiqNVacMhzuJ6lGCXtuHONzBqvPdYKrUi06pVQx9fe4S2WwDZRMIn/

IP´s
192[.]185[.]217[.]247
107[.]190[.]142[.]122

Localización
Houston, Texas, Estados Unidos
Orlando, Florida, estados Unidos

Ejemplo de Imagen del sitio


Peligroso | rigaan-bo.com/BCI/gjSE42vUQmxlDdPBefOpk3oX5n7r1YFRK9ls8TLy0CWwZtAbHGiqNVacMhzuJ6lGCXtuHONzBqvPdYKrUi06pVQx9fe4S2WwDZRMln/
Incógnito
Personas Preferencial Empresarios Empresas Wholesale Investor Relations
Sucursales Servicio al Cliente
Bci
Planes Tarjetas Créditos Seguros Inversiones Cuenta Vista Beneficios
Hazte Cliente
Banco en Línea
Ingresa a tu Banco en Línea
RUT
Clave
Ingresar
Solicitar clave de Internet
Olvidé mi clave de Internet
Ayuda en Línea con tu clave
Cuida tu clave personal
Renueva tu clave de seguridad por lo menos una vez al año y no la uses en otras cuentas (por ejemplo: e-mail).

Whois

```
soc@kali:~$ whois -h whois.google.com bcipersonas.com
Domain Name: bcipersonas.com
Registry Domain ID: 2434677607_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.google.com
Registrar URL: https://domains.google.com
Updated Date: 2019-09-18T18:16:06Z
Creation Date: 2019-09-18T18:16:04Z
Registrar Registration Expiration Date: 2020-09-18T18:16:04Z
Registrar: Google LLC
Registrar IANA ID: 895
Registrar Abuse Contact Email: registrar-abuse@google.com
Registrar Abuse Contact Phone: +1.8772376466
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Contact Privacy Inc. Customer 1245486931
Registrant Organization: Contact Privacy Inc. Customer 1245486931
Registrant Street: 96 Mowat Ave
Registrant City: Toronto
Registrant State/Province: ON
Registrant Postal Code: M4K 3K1
Registrant Country: CA
Registrant Phone: +1.4165385487
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: svqbvefyl4mi@contactprivacy.email
Registry Admin ID:
Admin Name: Contact Privacy Inc. Customer 1245486931
Admin Organization: Contact Privacy Inc. Customer 1245486931
Admin Street: 96 Mowat Ave
Admin City: Toronto
Admin State/Province: ON
Admin Postal Code: M4K 3K1
Admin Country: CA
Admin Phone: +1.4165385487
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: svqbvefyl4mi@contactprivacy.email
Registry Tech ID:
Tech Name: Contact Privacy Inc. Customer 1245486931
Tech Organization: Contact Privacy Inc. Customer 1245486931
Tech Street: 96 Mowat Ave
Tech City: Toronto
Tech State/Province: ON
Tech Postal Code: M4K 3K1
Tech Country: CA
Tech Phone: +1.4165385487
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: svqbvefyl4mi@contactprivacy.email
Name Server: NS-CLOUD-D1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D4.GOOGLEDOMAINS.COM
DNSSEC: unsigned
```

```
soc@kali:~$ whois -h whois.dynadot.com rigaan-bo.com
Domain Name: RIGAAN-BO.COM
Registry Domain ID: 2078017879_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http://www.dynadot.com
Updated Date: 2018-12-01T03:59:27.0Z
Creation Date: 2016-11-30T16:57:52.0Z
Registrar Registration Expiration Date: 2019-11-30T16:57:52.0Z
Registrar: DYNADOT LLC
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +1.6502620100
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: GcomPublicidad.com
Registrant Organization: GcomHosting.com
Registrant Street: Julio Leigue
Registrant Street: 8 de Diciembre #1020
Registrant City: Santa Cruz
Registrant Postal Code: 5742
Registrant Country: BO
Registrant Phone: +591.033310755
Registrant Email: dominios@gcomhosting.com
Registry Admin ID:
Admin Name: GcomPublicidad.com
Admin Organization: GcomHosting.com
Admin Street: Julio Leigue
Admin Street: 8 de Diciembre #1020
Admin City: Santa Cruz
Admin Postal Code: 5742
Admin Country: BO
Admin Phone: +591.033310755
Admin Email: dominios@gcomhosting.com
Registry Tech ID:
Tech Name: GcomPublicidad.com
Tech Organization: GcomHosting.com
Tech Street: Julio Leigue
Tech Street: 8 de Diciembre #1020
Tech City: Santa Cruz
Tech Postal Code: 5742
Tech Country: BO
Tech Phone: +591.033310755
Tech Email: dominios@gcomhosting.com
Name Server: dns1.gcomhosting.com
Name Server: dns2.gcomhosting.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: 2019.09.23 15:27:12 -03'00'