Alerta de seguridad informática	**8FFR-00024-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**22 de Agosto de 2019**
Última revisión	**22 de Agosto 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 un portal fraudulento asociado a una IP que suplanta el sitio web oficial del **bancochile.cl,** 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
spyinstructor[.]com/hhpdoejk5/wtuds/rvvgtgvt/LOA/index[.]php

https://www[.]kenyasweet[.]com/wp-content/uploads/2018/07/LOA/index[.]php

https://www[.]auto-usa[.]dp[.]ua/wp-includes/Text/cupos/R1/index[.]php/?&rpsnv=d6e3de36b09baee29613a44bada8dbc0d7202f31

IP´s
64.91.238.61
104.27.150.248
178.159.36.236
185.68.16.4

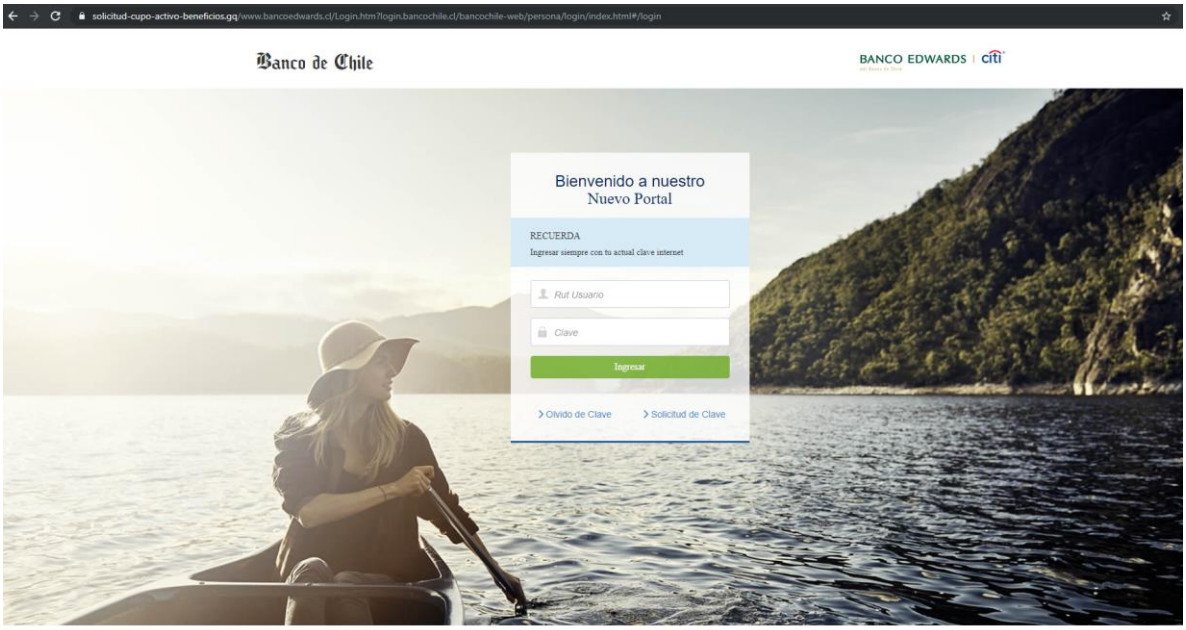
Localización
United States, San Francisco, California

Russian Federation, Moscow, Moskva

Ukraine, Kiev, Kyiv

Ejemplo de Imagen del sitio

Cometario: Al ingresar a las URL, esta se redirigen a la siguiente url: https://solicitud-cupo-activo-beneficios[.]gq/www[.]bancoedwards[.]cl/Login[.]htm?login[.]bancochile[.]cl/bancochile-web/persona/login/index[.]html#/login



Whois

```
Domain name:
   SOLICITUD-CUPO-ACTIVO-BENEFICIOS.GQ

Organisation:
   Equatorial Guinea Domains B.V.
   Dominio GQ administrator
   P.O. Box 11774
   1001 GT  Amsterdam
   Netherlands
   Phone: +31 20 5315725
   Fax: +31 20 5315721
   E-mail: abuse: abuse@freenom.com, copyright infringement: copyright@freenom.com

Domain Nameservers:
   NS02.FREENOM.COM
   NS03.FREENOM.COM
   NS01.FREENOM.COM
   NS04.FREENOM.COM


Your selected domain name is a Free Domain. That means that,
according to the terms and conditions of Free Domain domain names
the registrant is Equatorial Guinea Domains B.V.

Due to restrictions in Dominio GQ 's Privacy Statement personal information
about the user of the domain name cannot be released.

ABUSE OF A DOMAIN NAME
If you want to report abuse of this domain name, please send a
detailed email with your complaint to abuse@freenom.com.
In most cases Dominio GQ responds to abuse complaints within one business day.

COPYRIGHT INFRINGEMENT
If you want to report a case of copyright infringement, please send
an email to copyright@freenom.com, and include the full name and address of
your organization. Within 5 business days copyright infringement notices
will be investigated.

Record maintained by: Dominio GQ Domain Registry
```

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: 2019.08.22 18:15:46 -04'00'