Alerta de seguridad informática	8FFR-00113-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de Noviembre de 2019
Última revisión	16 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 37 portales fraudulentos asociado a una IP, los que suplantan el sitio web oficial de **Banco de Chile**, y que podrían 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
http[://]www-web-campana[.]ga/banconexion/
http[://]www-web-campana[.]ga/www[.]bancochile[.]cl/6iwxtqq4fb/7cnvt_persona/login_urb7/index/loginvzuv/
www-promo-cupo-avance[.]gq
www[.]www-promo-cupo-avance[.]gq
www-promo-avance[.]cf
www[.]www-promo-avance[.]cf
www-promo-avance[.]ga
www[.]www-promo-avance[.]ga
www-servicios-personas[.]gq
www[.]www-servicios-personas[.]gq
www[.]web-portal-avance[.]ga
web-portal-avance[.]ga
web-portal-avance[.]gq
www[.]web-portal-avance[.]gq
www[.]web-consulta-avance[.]ga
web-consulta-avance[.]ga
web-consulta-avance[.]gq
www[.]www-web-campana[.]ga
www-web-campana[.]ga
www-web-campana[.]cf
www[.]www-web-campana[.]cf
www-web-campana[.]gq
www[.]www-web-campana[.]gq
www-personas-portal[.]gq
www[.]web-portal-avance[.]cf
web-portal-avance[.]cf
www[.]www-personas-portal[.]gq
www[.]www-servicios-personas[.]cf
www-servicios-personas[.]cf
portal-web[.]cf
www[.]portal-web[.]cf
www-promo-cupo-avance[.]cf
www[.]www-promo-cupo-avance[.]cf
www-promo-cupo-avance[.]ga
www[.]www-promo-cupo-avance[.]ga
web-consulta-avance[.]cf
www[.]web-consulta-avance[.]cf

Domain www-web-campana.ga

www-web-campana / ga / Subdomains

TTL	value		
300	91.209.70.108		
300	ns04.freenom.com	Zones on DNS server	104.155.29.241
300	ns02.freenom.com	Zones on DNS server	52.19.156.76
300	ns03.freenom.com	Zones on DNS server	104.155.27.112
300	ns01.freenom.com	Zones on DNS server	54.171.131.39

300		
	Mname	ns01.freenom.com
	Rname	soa.freenom.com
	Serial number	1573063653
	Refresh	10800
	Retry	3600
	Expire	604800
	Minimum TTL	3600

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

Certificado

Criteria | Identity = 'www-web-campana.ga'

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2104746895	2019-11-13	2019-11-13	2020-02-11	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Au
2104746230	2019-11-13	2019-11-13	2020-02-11	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Au

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

IP´s

91.209.70.108

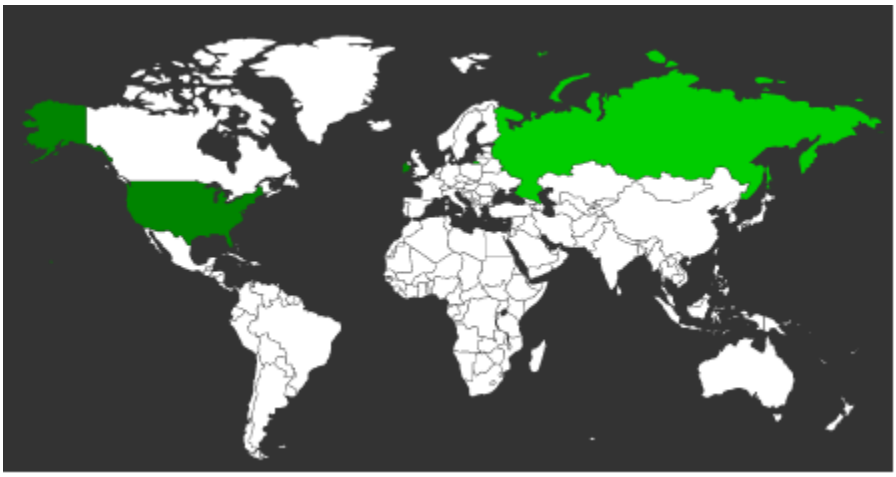
Domain www-web-campana.ga is located on IP address << 91.209.70.108 >>

Block start	91.209.70.0
End of block	91.209.70.255
Block size	256 Domains in block
Block name	PIHLTD
AS number	43317
Parent block	91.0.0.0 - 91.255.255.255
Organization	ORG-PIHL2-RIPE
City	Moscow
Region/State	Moskva
Country	RU , Russian Federation
Reg. date	2008-10-29
Host name	no record in reverse zone

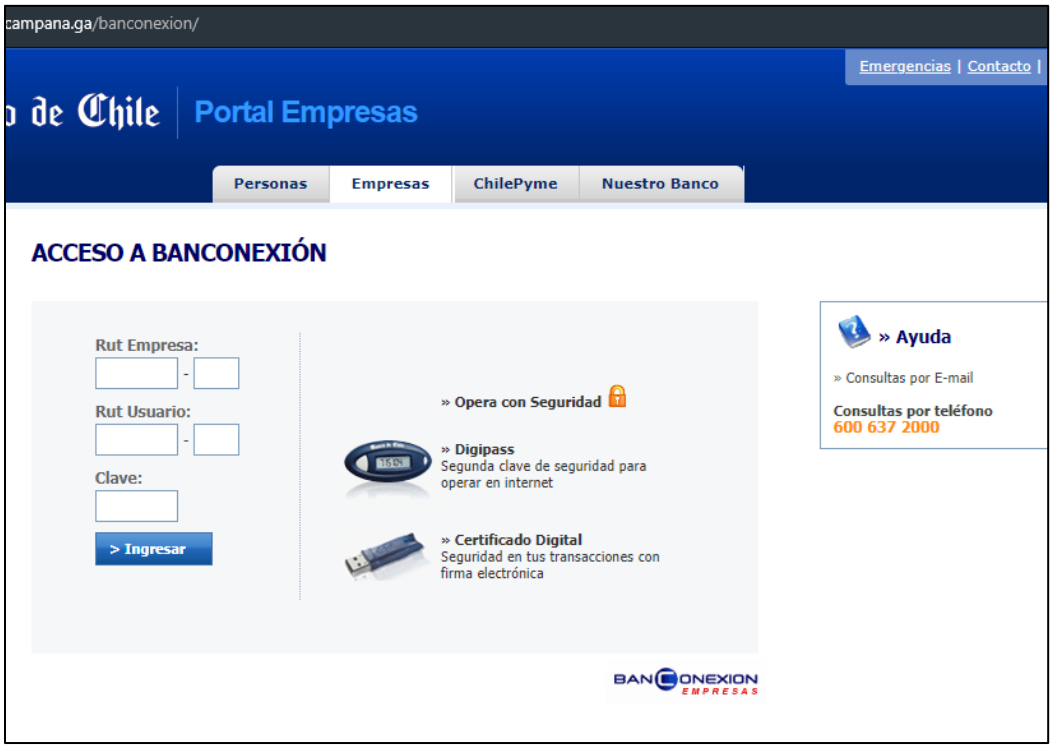
Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Chile

Localización

Moscow, Moskva, Federación Rusa



Imagen



Whois

```
   Domain name:
      WWW-WEB-CAMPANA.GA

   Organisation:
      Gabon TLD B.V.
      My GA 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@freeno
m.com

   Domain Nameservers:
      NS03.FREENOM.COM
      NS01.FREENOM.COM
      NS04.FREENOM.COM
      NS02.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 Gabon TLD B.V.

   Due to restrictions in My GA '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 My GA 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: My GA Domain Registry
```

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:       GA

organisation: Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)
address:      Cours Pasteur, (Immeuble de la Solde)
address:      BP: 798
address:      Libreville
address:      Gabon

contact:      administrative
name:         TLD Admin Contact
organisation: Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)
address:      Cours Pasteur, (Immeuble de la Solde)
address:      BP: 798
address:      Libreville
address:      Gabon
phone:        +241 01 76 32 49
e-mail:       cctldga-admin@nic.ga

contact:      technical
name:         Manager ICT
organisation: Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF)
address:      Cours Pasteur, (Immeuble de la Solde)
address:      BP: 798
address:      Libreville
address:      Gabon
phone:        +241 01 76 32 49
e-mail:       cctldga-tech@nic.ga

nserver:      A.NS.GA 185.21.168.49 2a04:1b00:c:0:0:0:0:1
nserver:      B.NS.GA 185.21.169.49 2a04:1b00:d:0:0:0:0:1
nserver:      C.NS.GA 185.21.170.49 2a04:1b00:e:0:0:0:0:1
nserver:      D.NS.GA 185.21.171.49 2a04:1b00:f:0:0:0:0:1

status:       ACTIVE

created:      1994-12-12
changed:      2018-11-28
source:       IANA
```

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: 2019.11.16 19:21:22 -03'00'