

Alerta de seguridad informática	8FFR-00088-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Octubre de 2019
Última revisión	14 de Octubre de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones 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 loC 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 loC 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 de **Banco 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

[http://confrimaciones\[.\]cf/www3\[.\]bancochile\[.\]cl/10girw19fd/sv2i4_persona/login_yw8o/index/loginl7t6/](http://confrimaciones[.]cf/www3[.]bancochile[.]cl/10girw19fd/sv2i4_persona/login_yw8o/index/loginl7t6/)

[http://confrimaciones\[.\]cf/www3\[.\]bancochile\[.\]cl/nj3tzuzyco/wyd4i_persona/login_5j4m/index/loginqrsm/](http://confrimaciones[.]cf/www3[.]bancochile[.]cl/nj3tzuzyco/wyd4i_persona/login_5j4m/index/loginqrsm/)

[http://confrimaciones\[.\]cf/www\[.\]bancochile\[.\]cl/hihgz1t69q/yumqv_persona/login_tu7g/index/logincdsq/](http://confrimaciones[.]cf/www[.]bancochile[.]cl/hihgz1t69q/yumqv_persona/login_tu7g/index/logincdsq/)

URL Asociado a la Campaña:

octubrecupones[.]cf

www[.]octubrecupones[.]cf

www[.]cupotemporal[.]ga

cupotemporal[.]ga

www[.]cupotemporal[.]cf

cupotemporal[.]cf

cupones[.]ga

cupones[.]gq

www[.]cupones[.]gq

cupones[.]cf

www[.]cupones[.]cf

www[.]confrimaciones[.]gq

confrimaciones[.]gq

confrimaciones[.]ga

www[.]confrimaciones[.]ga

www[.]confrimaciones[.]cf

confrimaciones[.]cf

Domain confrimaciones.cf																	
confrimaciones / cf / Subdomains																	
record type	TTL	value															
A	3600	91.234.99.106															
NS	300	ns04.freenom.com	Zones on DNS server 104.155.29.241														
NS	300	ns02.freenom.com	Zones on DNS server 52.19.156.76														
NS	300	ns03.freenom.com	Zones on DNS server 104.155.27.112														
NS	300	ns01.freenom.com	Zones on DNS server 54.171.131.39														
SOA	300	<table border="1"> <tr> <td>Mname</td> <td>ns01.freenom.com</td> </tr> <tr> <td>Rname</td> <td>soa.freenom.com</td> </tr> <tr> <td>Serial number</td> <td>1570725490</td> </tr> <tr> <td>Refresh</td> <td>10800</td> </tr> <tr> <td>Retry</td> <td>3600</td> </tr> <tr> <td>Expire</td> <td>604800</td> </tr> <tr> <td>Minimum TTL</td> <td>3600</td> </tr> </table>		Mname	ns01.freenom.com	Rname	soa.freenom.com	Serial number	1570725490	Refresh	10800	Retry	3600	Expire	604800	Minimum TTL	3600
Mname	ns01.freenom.com																
Rname	soa.freenom.com																
Serial number	1570725490																
Refresh	10800																
Retry	3600																
Expire	604800																
Minimum TTL	3600																

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

Certificado

Certificates	crt.sh ID	Logged At ↑	Not Before	Not After	Issuer Name
	1981204067	2019-10-10	2019-10-10	2020-01-08	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
	1981203974	2019-10-10	2019-10-10	2020-01-08	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"

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

IP's

91[.]234[.]99[.]106

Domain confrimaciones.cf is located on IP address << 91.234.99.106 >>	
Block start	91.234.99.0
End of block	91.234.99.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	48666
Parent block	91.0.0.0 - 91.255.255.255
Organization	ORG-PIHL2-RIPE
City	Kiev
Region/State	Kyiv
Country	 UA , Ukraine
Reg. date	2011-12-30
Host name	no record in reverse zone
Domain count	> = 3 Servers around
Domains	<ul style="list-style-type: none"> 1  confrimaciones.cf 2  digitales-aumento-cupo.cf 3  octubre.ml

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

Localización

Amsterdam, Noord-Holland, Países Bajos

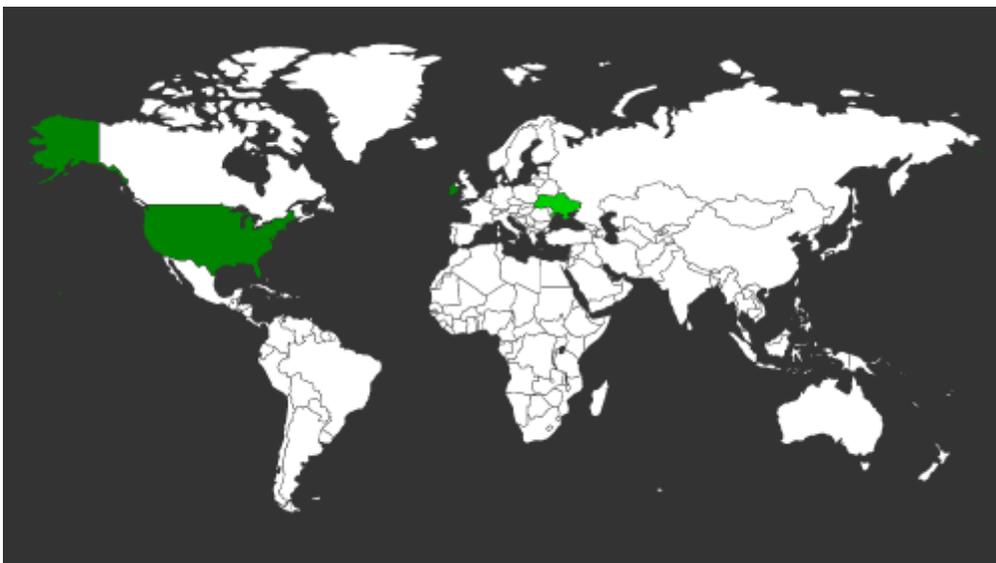
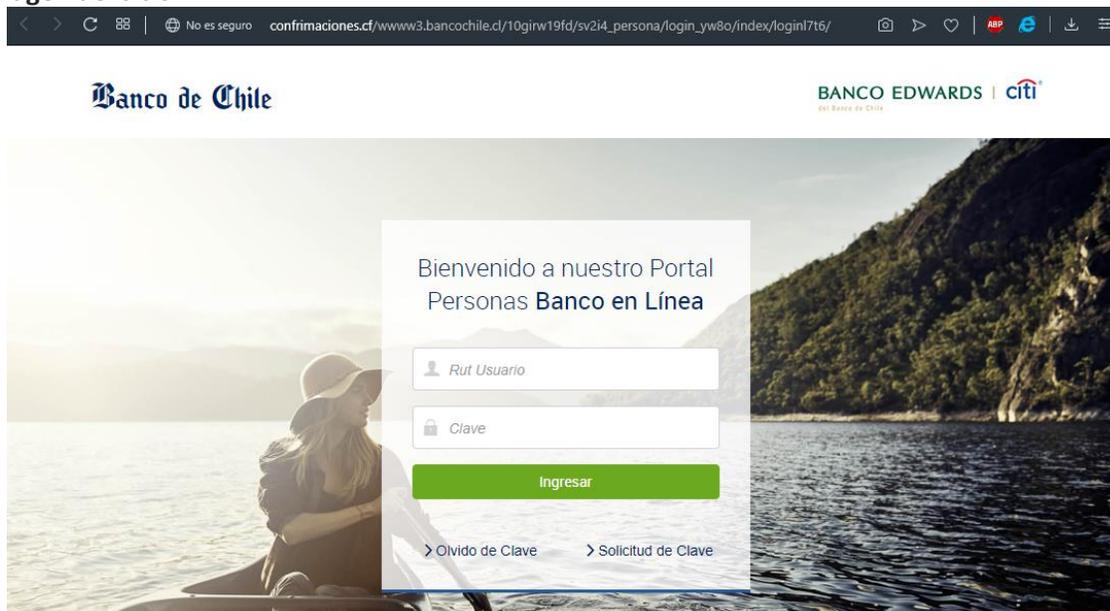


Imagen del sitio



Whois

```
soc@ITQ-ivps2:~$ whois confrimaciones.cf

Domain name:
  CONFRIMACIONES.CF

Organisation:
  Centrafrique TLD B.V.
  Dot CF 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:
  NS01.FREENOM.COM
  NS02.FREENOM.COM
  NS03.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 Centrafrique TLD B.V.

Due to restrictions in Dot CF '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 Dot CF 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: Dot CF 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