Alerta de seguridad informática	8FFR20-00212-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de febrero de 2020
Última revisión	08 de febrero de 2020

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 dos IPs que suplantan el sitio web oficial de Banco de Chile, los cuales 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

URLs

bancachileperersonas-cl[.]website/bancochile-web/persona/login/index[.]html#/login
bancachileperersonas-cl[.]website
bancaschile-cl[.]regtistrerut[.]ml/persona/login/

Domain bancachileperersonas-cl.website

bancachileperersonas-cl / website / Subdomains

record type	TTL	value		
A	1200	199.188.206.83		
NS	1800000	dns1.namecheaphosting.com	Zones on DNS server	156.154.132.200
NS	1800000	dns2.namecheaphosting.com	Zones on DNS server	156.154.133.200
MX	1200	0 mail.bancachileperersonas-cl.website		
TXT	1200	v=spf1 +a +mx +ip4:199.188.206.50 include:spf.web-hosting.com ~all		

SOA	1800000		
		Mname	dns1.namecheaphosting.com
		Rname	cpanel.tech.namecheap.com
		Serial number	1580938517
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	86400

Domain regtistrerut.ml

regtistrerut / ml / Subdomains

record type	TTL	value		
A	14400	192.185.39.252		
NS	86400	ns8196.hostgator.com	Zones on DNS server	192.185.39.27
NS	86400	ns8195.hostgator.com	Zones on DNS server	192.185.39.26
MX	14400	0 mail.regtistrerut.ml		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		

SOA	86400		
		Mname	ns8195.hostgator.com
		Rname	root.gator4098.hostgator.com
		Serial number	2020020606
		Refresh	86400
		Retry	7200
		Expire	3600000
		Minimum TTL	86400

Ilustración 1 Dominio donde se aloja URL del Banco de Chile falso y DNS que utiliza

Certificados

Subject DN	CN=bancachileperersonas-cl.website
Issuer DN	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
Serial	242927648738674641676822470000371890909
Validity	2020-02-05 00:00:00 **to** 2021-02-04 23:59:59 (365 days, 23:59:59)
Names	bancachileperersonas-cl.website www.bancachileperersonas-cl.website

Subject DN	CN=bancaschile-cl.regtistrerut.ml
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	308541983710689761443787467402451243996938
Validity	2020-02-06 18:00:35 **to** 2020-05-06 18:00:35 (90 days, 0:00:00)
Names	bancaschile-cl.regtistrerut.ml www.bancaschile-cl.regtistrerut.ml

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

IPs

199.188.206.83

192.185.39.252

Domain bancachileperersonas-cl.website is located on IP address
<< 199.188.206.83 >>

Block start	199.188.200.0
End of block	199.188.207.255
Block size	2048 Domains in block
Block name	NCNET-1
AS number	22612
Parent block	199.0.0.0 - 199.255.255.255
Organization	Namecheap, Inc.
City	Atlanta
Region/State	Georgia
Country	US , United States
Reg. date	2011-08-03
Host name	server270-5.web-hosting.com

Domain bancaschile-cl.regtistrerut.ml is located on IP address << 192.185.39.252 >>

Block start	192.185.0.0
End of block	192.185.255.255
Block size	65536 Domains in block
Block name	HGBLOCK-10
AS number	46606
Parent block	192.0.0.0 - 192.255.255.255
Organization	WEBSITEWELCOME.COM
City	Houston
Region/State	Texas
Country	US , United States
Reg. date	2013-07-22
Host name	no record
Web server	nginx/1.10.2
Domain count	>= 661 Servers around
Domains	1 10000in30days.com 2 10kliveclass.org 3 10kwithvince.com 4 12jewels.com 5 25travels.com

Ilustración 3 IP de origen donde se aloja sitio falso del Banco de Chile

Localización

USA, Atlanta, Georgia
USA, Provo, Utah

Location	Los Angeles, California, United States (US)
Latitude and Longitude	34.03, -118.43

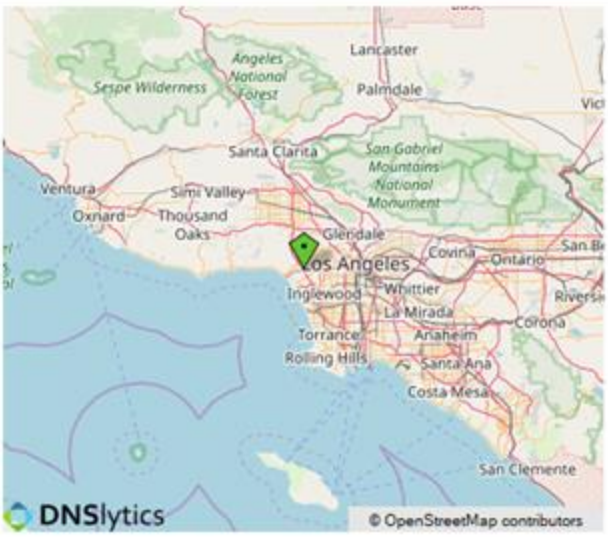
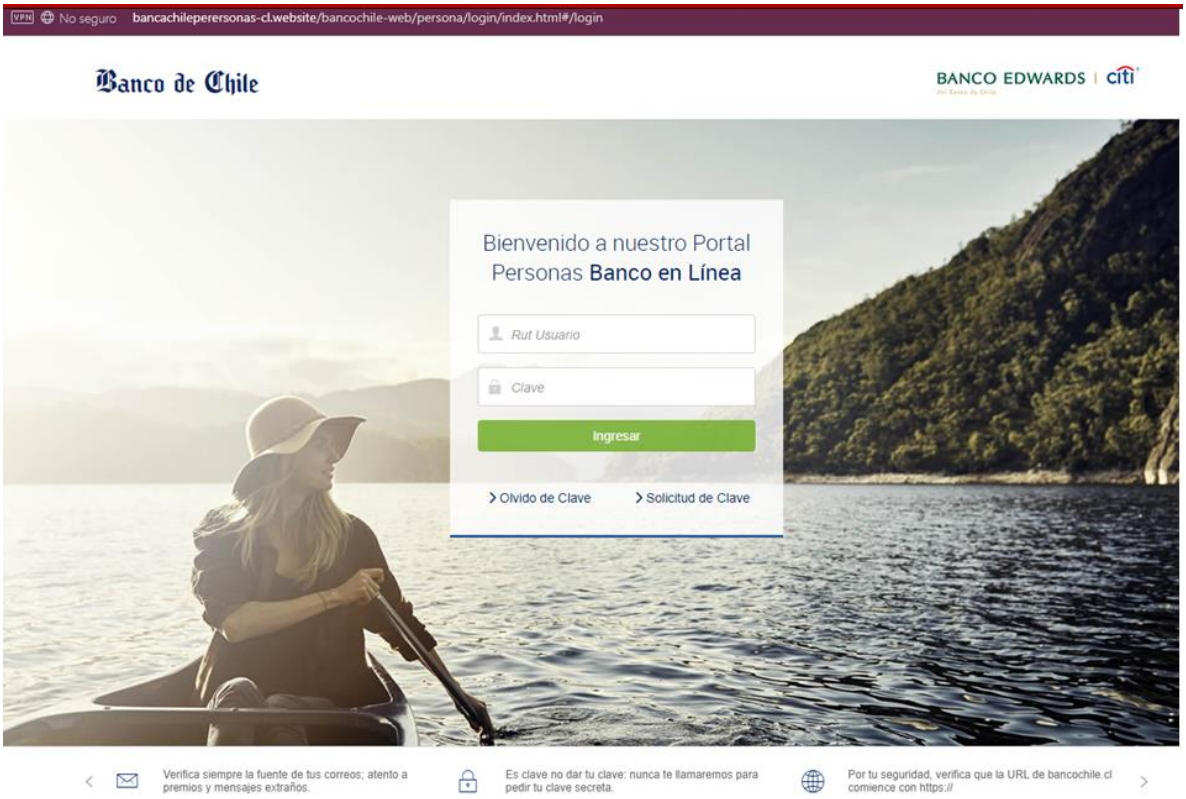
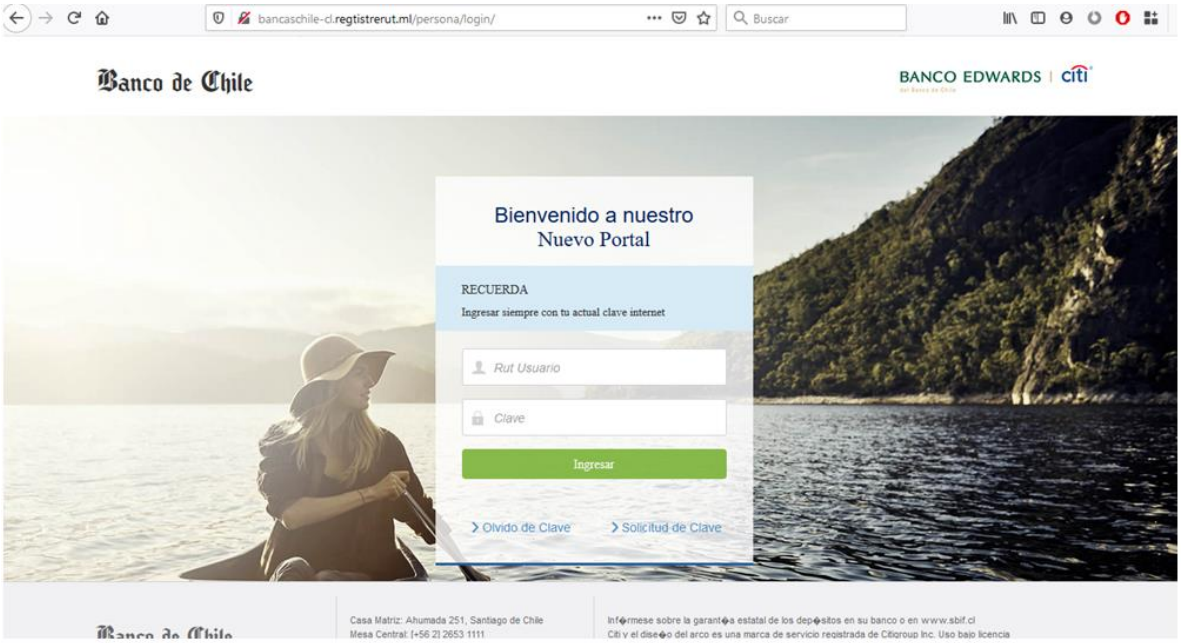


Imagen del sitio





Whois

```
Domain Name: BANCACHILEPERERSONAS-CL.WEBSITE
Registry Domain ID: D169685071-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: https://namecheap.com
Updated Date: 2020-02-05T21:34:59.0Z
Creation Date: 2020-02-05T21:34:47.0Z
Registry Expiry Date: 2021-02-05T23:59:59.0Z
Registrar: Namecheap
Registrar IANA ID: 1068
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: WhoisGuard, Inc.
Registrant State/Province: Panama
Registrant Country: PA
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: DNS1.NAMECHEAPHOSTING.COM
Name Server: DNS2.NAMECHEAPHOSTING.COM
DNSSEC: unsigned
```

```
Domain name:
   REGTISTRERUT.ML

Organisation:
   Mali Dili B.V.
   Point ML 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:
   NS8195.HOSTGATOR.COM
   NS8196.HOSTGATOR.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 Mali Dili B.V.

Due to restrictions in Point ML '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 Point ML 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: Point ML 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: 2020.02.08 21:52:01 -03'00'