Alerta de seguridad informática	**8FFR-00099-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**25 de Octubre de 2019**
Última revisión	**25 de Octubre 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 de Banco de 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
https[://]www[.]bancochile[.]store/mobile/choose[.]php

URL Sitio Clonado:
http[://]validoschile[.]gq/www[.]bancochile[.]cl/7qiasnojeg/hc33i_persona/login_8mda/index/loginjdca/
http[://]validoschile[.]gq/www[.]bancoedwards[.]cl/6fsyq0i34e/v1a1o_persona/login_3bl7/index/login1ojc/
http[://]validoschile[.]gq/www3[.]bancochile[.]cl/wlrril4cl6/ua3r9_persona/login_qlf1/index/logininf48/
http[://]validoschile[.]gq/www3[.]bancoedwards[.]cl/u94atrlok1/y87k0_persona/login_7qx2/index/loginrs6h/
http[://]validoschile[.]gq/wwww3[.]bancochile[.]cl/dq0kon8v51/6de1d_persona/login_stly/index/loginrc4g/

Domain www.bancochile.store

www / bancochile / store / Subdomains

record type	TTL	value	
CNAME	900	bancochile.store	80.211.58.197

Domain validoschile.gq

validoschile / gq / 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	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1571079893	
		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.bancochile.store'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2025761594	2019-10-21	2019-10-21	2020-01-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2021064513	2019-10-21	2019-10-21	2020-01-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria	Identity = 'validoschile.gq'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2006506438	2019-10-16	2019-10-16	2020-01-14	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2006506307	2019-10-16	2019-10-16	2020-01-14	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
80[.]211[.]58[.]197
91[.]234[.]99[.]106

Domain www.bancochile.store is located on IP address << 80.211.58.197 >>

Block start	80.211.58.0
End of block	80.211.58.255
Block size	256 Domains in block
Block name	ARUBA-NET
AS number	31034
Parent block	80.211.0.0 - 80.211.127.255
Organization	Aruba S.p.A. - Cloud Services DC1
City	Arezzo
Region/State	Toscana
Country	IT , Italy
Host name	host197-58-211-80.serverdedicati.aruba.it
Domain count	>= 2 Servers around
Domains	1 www.bancochile.store 2 www.bancochile.tech

Domain validoschile.gq 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	Amsterdam
Region/State	Noord-Holland
Country	NL , Netherlands
Reg. date	2011-12-30
Host name	no record in reverse zone
Domain count	>= 9 Servers around

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

Localización
Arezzo, Toscana, Italia
Amsterdam, Noord-Holland, Países Bajos

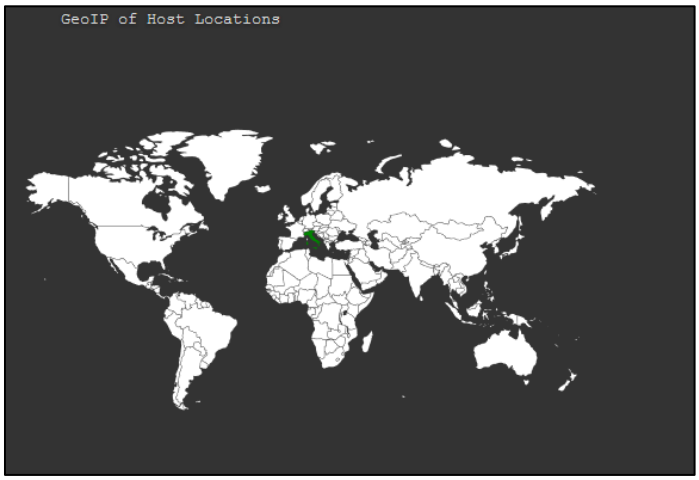
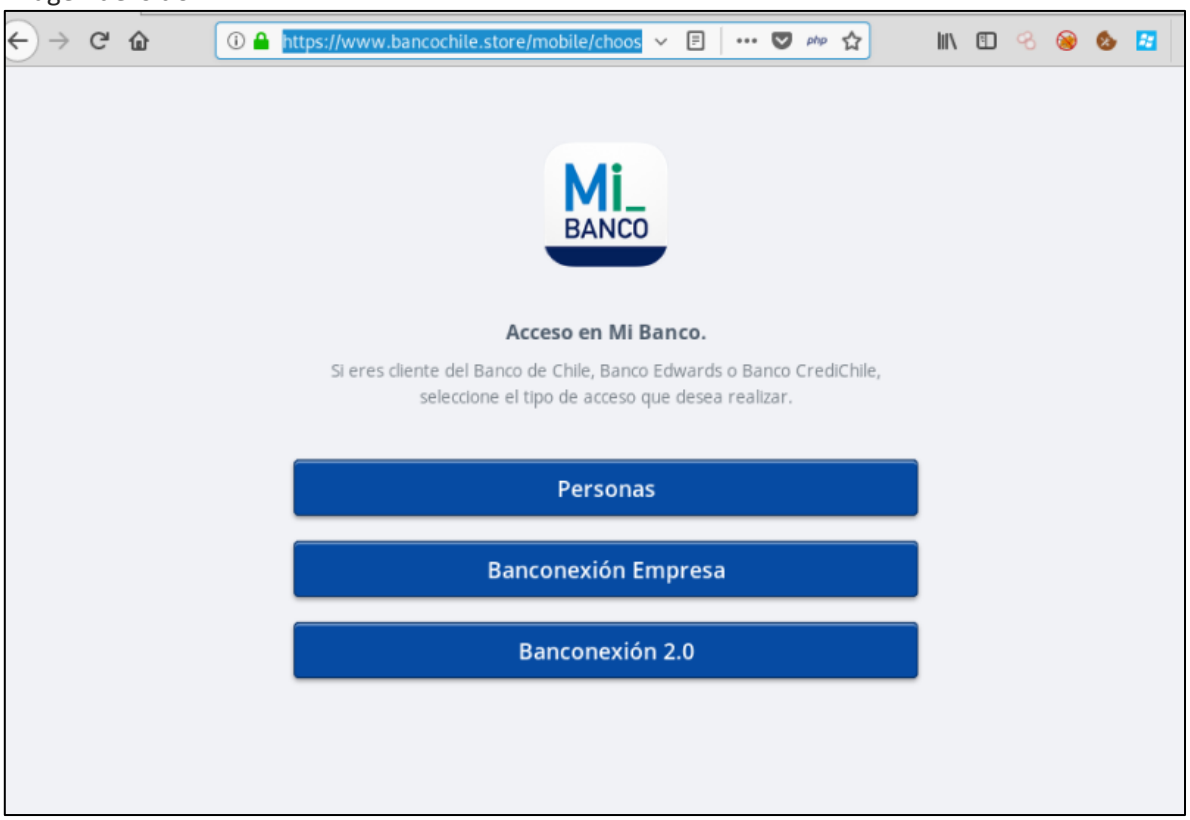
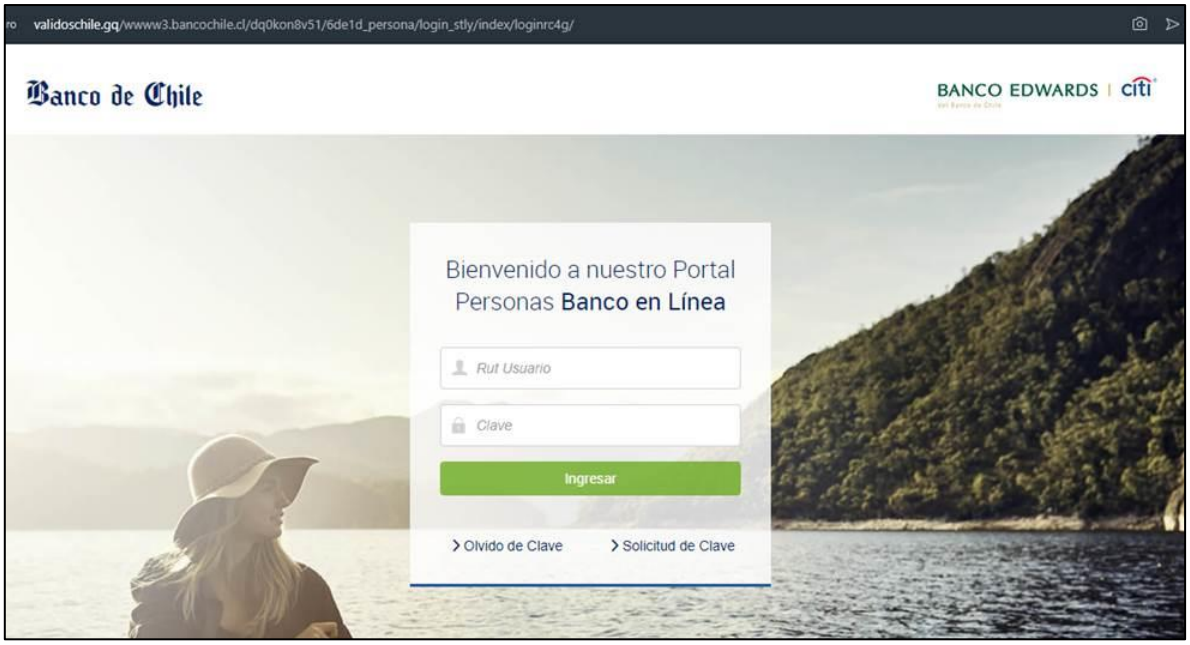


Imagen del sitio





Whois

```
Domain Name: bancochile.store
Registry Domain ID: D136545465-CNIC
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-10-24T18:33:48.00Z
Creation Date: 2019-10-20T17:53:00.00Z
Registrar Registration Expiration Date: 2020-10-20T17:53:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientHold https://www.icann.org/epp#clientHold
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransfer
Prohibited
Domain Status: addPeriod https://www.icann.org/epp#addPeriod
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street:
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: PARA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: BR
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/8eed537b-633b-4016-9604-c3c39
1a5ec25
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street:
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street:
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Name Server: NS1.AMENWORLD.COM
Name Server: NS2.AMENWORLD.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: 2019.10.25 11:04:57 -03'00'