Alerta de seguridad cibernética	8FFR20-00341-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de abril de 2020
Última revisión	16 de abril 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 tres portales fraudulentos asociados a tres IPs que suplantan 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 COMPROMISO

URL
pre-covid-banchile[.]net
bancochile-portal[.]eu
pre-covid[.]nl

IP
178[.]159[.]36[.]139
178[.]159[.]36[.]139
178[.]159[.]36[.]139

DOMINIOS DONDE SE ALOJA URL

Domain pre-covid-banchile.net

pre-covid-banchile / net / Subdomains

record type	TTL	value		
A	3600	178.159.36.139		
NS	300	ns02.freenom.com	Zones on DNS server	52.19.156.76
NS	300	ns04.freenom.com	Zones on DNS server	104.155.29.241
NS	300	ns01.freenom.com	Zones on DNS server	54.171.131.39
NS	300	ns03.freenom.com	Zones on DNS server	104.155.27.112
SOA	300	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1586924054	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

Domain bancochile-portal.eu

bancochile-portal / eu / Subdomains

record type	TTL	value		
A	3600	178.159.36.139		
NS	300	ns01.freenom.com	Zones on DNS server	54.171.131.39
NS	300	ns03.freenom.com	Zones on DNS server	104.155.27.112
NS	300	ns02.freenom.com	Zones on DNS server	52.19.156.76
NS	300	ns04.freenom.com	Zones on DNS server	104.155.29.241
SOA	300	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1586883176	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

Domain pre-covid.nl

pre-covid / nl / Subdomains

record type	TTL	value		
A	3600	178.159.36.139		
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
NS	300	ns04.freenom.com	Zones on DNS server	104.155.29.241
SOA	300	Mname	ns01.freenom.com	
		Rname	soa.freenom.com	
		Serial number	1586924067	
		Refresh	10800	
		Retry	3600	
		Expire	604800	
		Minimum TTL	3600	

CERTIFICADOS

Subject DN	CN=pre-covid-banchile.net
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	304456353355513992534390205681542483598656
Validity	2020-04-15 11:27:24 **to** 2020-07-14 11:27:24 (90 days, 0:00:00)
Names	pre-covid-banchile.net www.pre-covid-banchile.net

Subject DN	CN=bancochile-portal.eu
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	378369503376576757431020750275501172448586
Validity	2020-04-15 00:55:27 **to** 2020-07-14 00:55:27 (90 days, 0:00:00)
Names	bancochile-portal.eu www.bancochile-portal.eu

Subject DN	CN=pre-covid.nl
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	285072335209467150903908259219260430353649
Validity	2020-04-15 04:18:18 **to** 2020-07-14 04:18:18 (90 days, 0:00:00)
Names	pre-covid.nl www.pre-covid.nl

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain pre-covid-banchile.net is located on IP address << 178.159.36.139 >>

Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	35196
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE

Domain bancochile-portal.eu is located on IP address << 178.159.36.139 >>

Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	35196
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE

Domain pre-covid.nl is located on IP address << 178.159.36.139 >>

Block start	178.159.36.0
End of block	178.159.36.255
Block size	256 Domains in block
Block name	PrivateInternetHosting
AS number	35196
Parent block	178.0.0.0 - 178.255.255.255
Organization	ORG-PIHL2-RIPE

LOCALIZACIÓN

Moscú, Federación Rusa

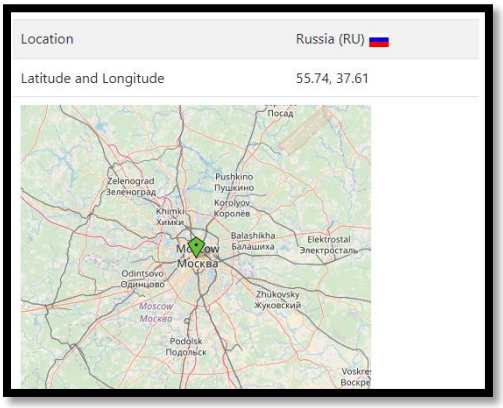
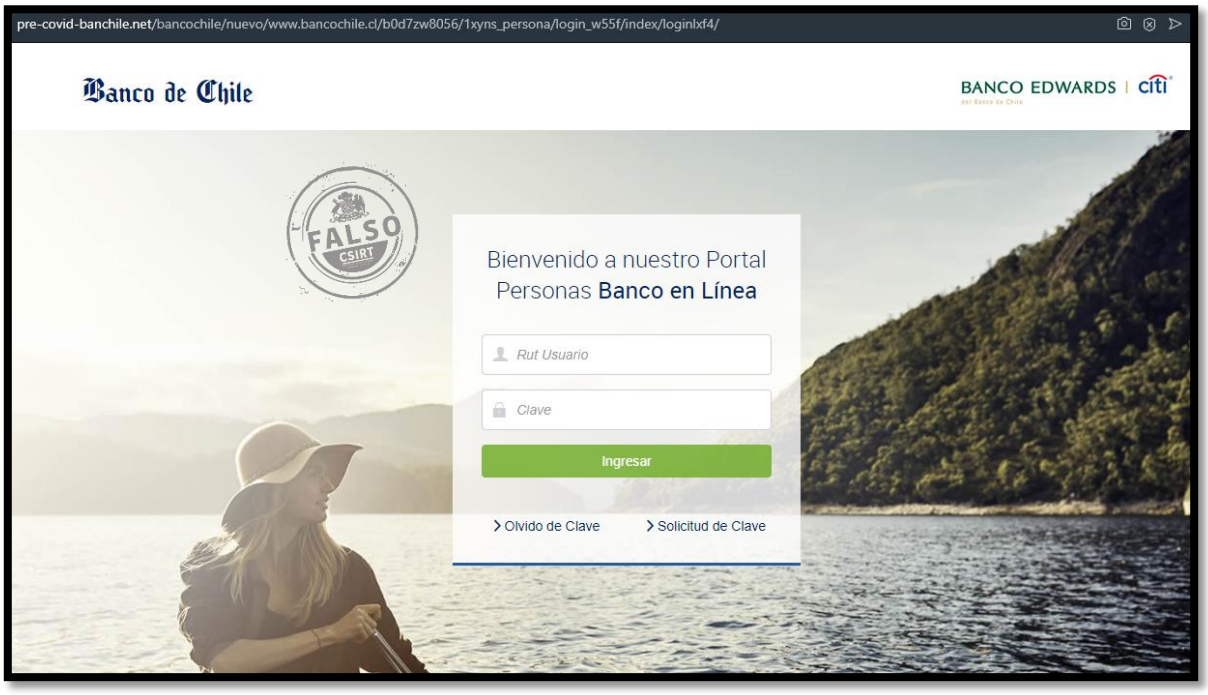
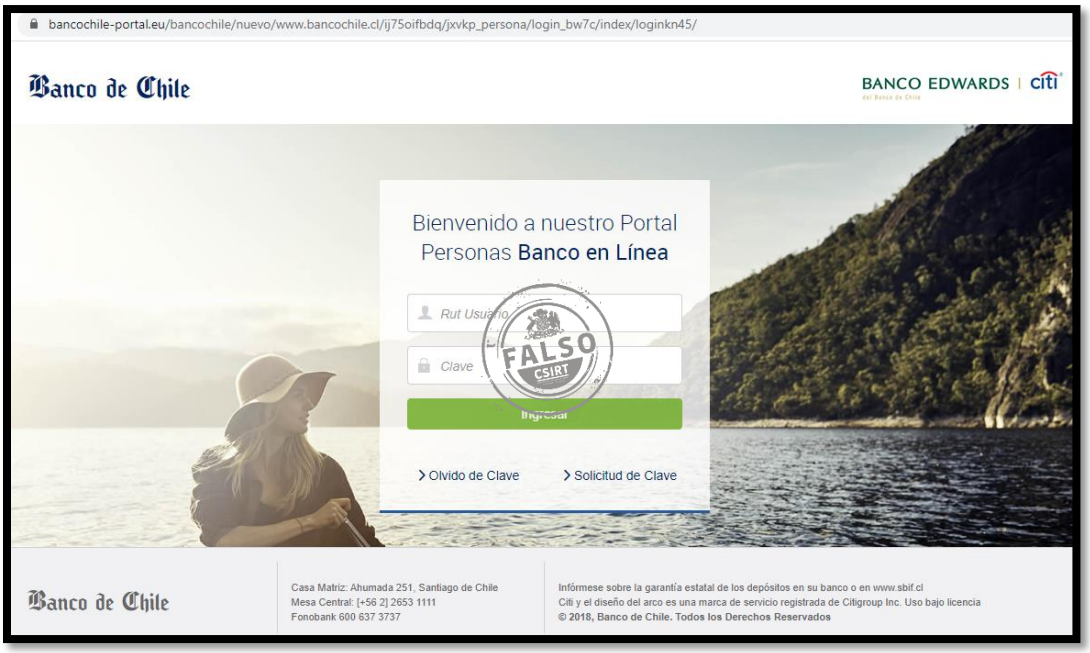
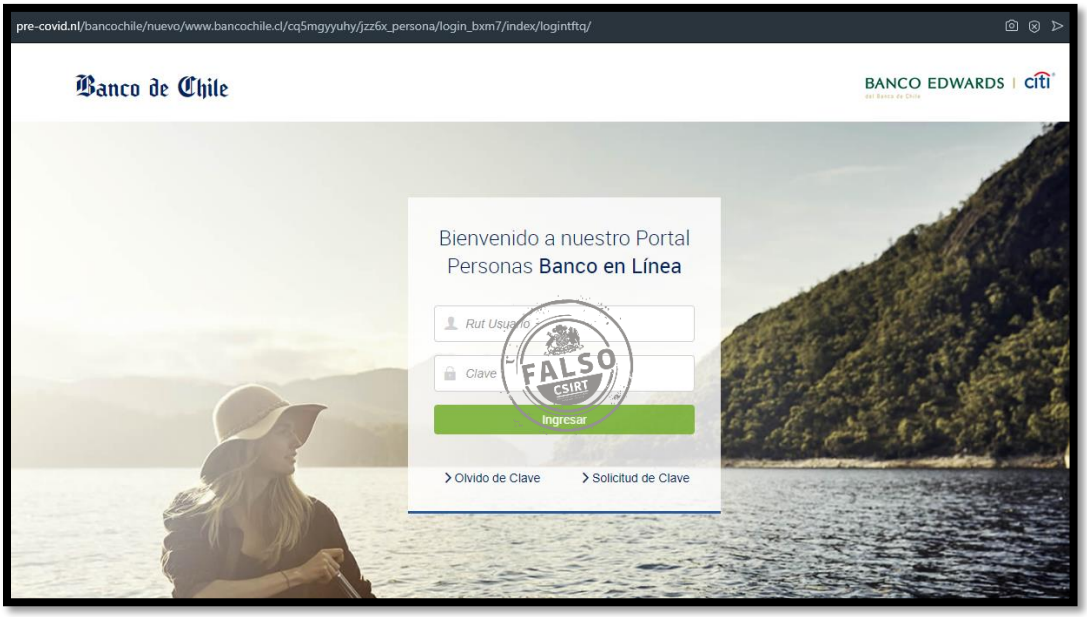


IMAGEN DEL SITIO




bancochile-portal.eu/bancochile/nuevo/www.bancochile.cl/ij75oifbdq/jxvkp_persona/login_bw7c/index/loginkn45/
Banco de Chile
BANCO EDWARDS | citi
Bienvenido a nuestro Portal
Personas Banco en Línea
Rut Usuario
Clave
FALSO
CSIRT
Ingresar
Olvido de Clave
Solicitud de Clave
Banco de Chile
Casa Matriz: Ahumada 251, Santiago de Chile
Mesa Central: [+56 2] 2653 1111
Fonobank 600 637 3737
Infórmese sobre la garantía estatal de los depósitos en su banco o en www.sbif.cl
Citi y el diseño del arco es una marca de servicio registrada de Citigroup Inc. Uso bajo licencia
© 2018, Banco de Chile. Todos los Derechos Reservados


pre-covid.nl/bancochile/nuevo/www.bancochile.cl/cq5mgyyuhy/jzz6x_persona/login_bxm7/index/logintftq/
Banco de Chile
BANCO EDWARDS | citi
Bienvenido a nuestro Portal
Personas Banco en Línea
Rut Usuario
Clave
FALSO
CSIRT
Ingresar
Olvido de Clave
Solicitud de Clave

WHOIS

```
Domain Name: PRE-COVID-BANCHILE.NET
Registry Domain ID: 2514903639_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.freenom.com
Registrar URL: www.freenom.com
Updated Date: 2020-04-15T04:03:10Z
Creation Date: 2020-04-15T04:03:10Z
Registrar Registration Expiration Date: 2021-04-15T04:03:10Z
Registrar: OpentTLD B.V.
Registrar IANA ID: 1666
Registrar Abuse Contact Email: abuse@freenom.com
Registrar Abuse Contact Phone: +31.205315726
Domain Status: clientTransferProhibited - http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: NL-NH
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: NL
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact via https://send-message.ispapi.net/pre-covid-banchile.net/registrant
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
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: +31.20.5315721
Admin Fax Ext:
Admin Email: contact via https://send-message.ispapi.net/pre-covid-banchile.net/admin
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
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:
Tech Fax Ext:
Tech Email: contact via https://send-message.ispapi.net/pre-covid-banchile.net/tech
Name Server: ns01.freenom.com 54.171.131.39
Name Server: ns02.freenom.com 52.19.156.76
Name Server: ns03.freenom.com 104.155.27.112
Name Server: ns04.freenom.com 104.155.29.241
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
```

```
Domain: bancochile-portal.eu
Script: LATIN

Registrant:
        NOT DISCLOSED!
        Visit www.eurid.eu for webbased WHOIS.

On-site(s):
        NOT DISCLOSED!
        Visit www.eurid.eu for webbased WHOIS.

Registrar:
        Name: OpenTLD B.V.
        Website: http://www.freenom.com

Name servers:
        ns01.freenom.com
        ns02.freenom.com
        ns04.freenom.com
        ns03.freenom.com
```

```
Domain name: pre-covid.nl
Status:      active

Registrar:
   OpenTLD B.V.
   Keizersgracht 213
   1016DT AMSTERDAM
   Netherlands

Abuse Contact:

Creation Date: 2020-04-15

DNSSEC:      no

Domain nameservers:
   ns01.freenom.com
   ns02.freenom.com
   ns03.freenom.com
   ns04.freenom.com

Record maintained by: NL 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: 2020.04.16 10:40:06 -04'00'