

Alerta de seguridad cibernética	8FFR20-00316-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de abril de 2020
Última revisión	07 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 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 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 COMPROMISO

URL
servicios-movil[.]bchileportal[.]com

IP
195[.]123[.]208[.]185

DOMINIOS DONDE SE ALOJA URL


Domain servicios-movil.bchileportal.com ⓘ			
servicios-movil / bchileportal / com /  Subdomains			
record type	TTL	value	
A	14400	195.123.208.185	

Domain bchileportal.com ⓘ																	
bchileportal / com /  Subdomains																	
record type	TTL	value															
A	14400	195.123.208.185															
NS	86400	ns1.bchileportal.com	 Zones on DNS server 195.123.208.185														
NS	86400	ns2.bchileportal.com	 Zones on DNS server 195.123.208.185														
MX	14400	0 bchileportal.com															
TXT	14400	v=spf1 +a +mx +ip4:195.123.208.185 ~all															
SOA	86400	<table border="1"> <tr> <td>Mname</td> <td>ns1.bchileportal.com</td> </tr> <tr> <td>Rname</td> <td>root.bastx.vps.com</td> </tr> <tr> <td>Serial number</td> <td>2020040607</td> </tr> <tr> <td>Refresh</td> <td>3600</td> </tr> <tr> <td>Retry</td> <td>1800</td> </tr> <tr> <td>Expire</td> <td>1209600</td> </tr> <tr> <td>Minimum TTL</td> <td>86400</td> </tr> </table>		Mname	ns1.bchileportal.com	Rname	root.bastx.vps.com	Serial number	2020040607	Refresh	3600	Retry	1800	Expire	1209600	Minimum TTL	86400
Mname	ns1.bchileportal.com																
Rname	root.bastx.vps.com																
Serial number	2020040607																
Refresh	3600																
Retry	1800																
Expire	1209600																
Minimum TTL	86400																

CERTIFICADOS


crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2671739897	2020-04-06	2020-04-06	2020-07-05	servicios-movil.bchileportal.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2671878441	2020-04-06	2020-04-06	2020-07-05	servicios-movil.bchileportal.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2671730922	2020-04-06	2020-04-06	2020-07-05	servicios-movil.bchileportal.com www.servicios-movil.bchileportal.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
2671730940	2020-04-06	2020-04-06	2020-07-05	servicios-movil.bchileportal.com www.servicios-movil.bchileportal.com	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"


IP DE ORIGEN DONDE SE ALOJA SITIO

<p>Domain <u>servicios-movil.bchileportal.com</u> is located on IP address</p> <p><< 195.123.208.185 >></p>	
Block start	195.123.208.0
End of block	195.123.215.255
Block size	2048  Domains in block
Block name	GF-RIX-NET
AS number	50979
Parent block	195.123.208.0 - 195.123.247.255
Organization	* * As ISP we provide hosting, virtual and dedicated servers. * * Those services are self managed by our customers * therefore, we are not us

LOCALIZACIÓN

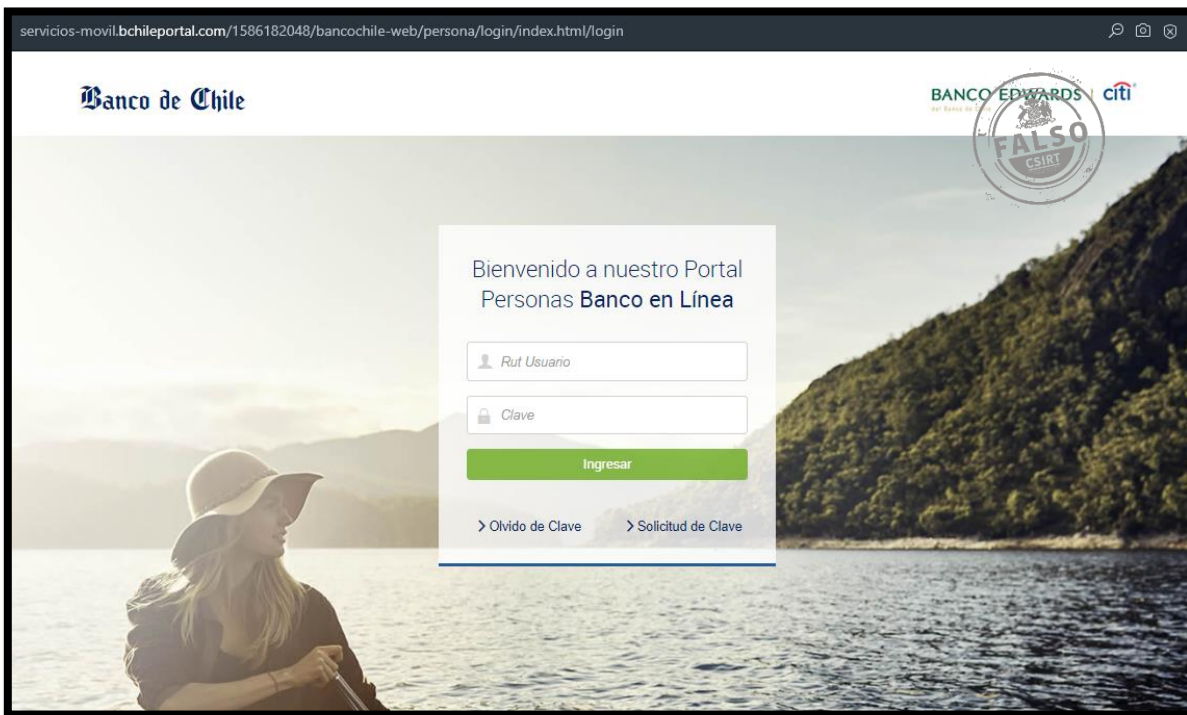
Letonia

Location	Latvia (LV) 
Latitude and Longitude	57, 25



The map displays the geographical context of the location in Latvia. It shows the Gauja National Park and the Vidzeme region. A green pin is placed on the map to indicate the specific location. The city of Riga is also visible on the left side of the map.

IMAGEN DEL SITIO



WHOIS

```
Domain Name: BCHILEPORTAL.COM
Registry Domain ID: 2511208328_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.domain.com
Registrar URL: www.domain.com
Updated Date: 2020-04-05T17:18:18
Creation Date: 2020-04-05T17:08:20
Registrar Registration Expiration Date: 2021-04-05T17:08:20
Registrar: Domain.com, LLC
Registrar IANA ID: 886
Reseller: Domain.com
Domain Status:
Registry Registrant ID:
Registrant Name: Domain Privacy Service FBO Registrant.
Registrant Organization: Domain Privacy Service FBO Registrant.
Registrant Street: 10 Corporate Drive
Registrant City: Burlington
Registrant State/Province: MA
Registrant Postal Code: 01803
Registrant Country: US
Registrant Phone: +1.6027165339
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: bchileportal.com@domainprivacygroup.com
Registry Admin ID:
Admin Name: Domain Privacy Service FBO Registrant.
Admin Organization: Domain Privacy Service FBO Registrant.
Admin Street: 10 Corporate Drive
Admin City: Burlington
Admin State/Province: MA
Admin Postal Code: 01803
Admin Country: US
Admin Phone: +1.6027165339
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: bchileportal.com@domainprivacygroup.com
Registry Tech ID:
Tech Name: Domain Privacy Service FBO Registrant.
Tech Organization: Domain Privacy Service FBO Registrant.
Tech Street: 10 Corporate Drive
Tech City: Burlington
Tech State/Province: MA
Tech Postal Code: 01803
Tech Country: US
Tech Phone: +1.6027165339
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: bchileportal.com@domainprivacygroup.com
Name Server: ns2.domain.com
Name Server: ns1.domain.com
DNSSEC: unsigned
Registrar Abuse Contact Email: compliance@domain-inc.net
Registrar Abuse Contact Phone: +1.6027165396
```

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.