Alerta de seguridad cibernética	8FFR20-00301-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de abril de 2020
Última revisión	02 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 dos portales fraudulentos asociados a una IP 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
portalbncochile-cl[.]xyz
ayudas-valida-aumento-personas-chile[.]ml

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

DOMINIOS DONDE SE ALOJA URL

Domain portalbncochile-cl.xyz

portalbncochile-cl / xyz / Subdomains

record type	TTL	value		
A	300	178.159.36.139		
NS	1800	dns1.registrar-servers.com	Zones on DNS server	156.154.132.200
NS	1800	dns2.registrar-servers.com	Zones on DNS server	156.154.133.200
MX	1800	10 eforward1.registrar-servers.com		162.255.118.51
MX	1800	10 eforward2.registrar-servers.com		162.255.118.52
MX	1800	10 eforward3.registrar-servers.com		162.255.118.51
MX	1800	15 eforward4.registrar-servers.com		162.255.118.61
MX	1800	20 eforward5.registrar-servers.com		162.255.118.62
TXT	1800	v=spf1 include:spf.efwd.registrar-servers.com ~all		
SOA	3601	Mname: dns1.registrar-servers.com Rname: hostmaster.registrar-servers.com Serial number: 1585595030 Refresh: 43200 Retry: 3600 Expire: 604800 Minimum TTL: 3601		

Domain ayudas-valida-aumento-personas-chile.ml

ayudas-valida-aumento-personas-chile / ml / Subdomains

record type	TTL	value
No records found		

CERTIFICADOS

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2646367311	2020-03-30	2020-03-30	2020-06-28	portalbncochile-cl.xyz	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2646368053	2020-03-30	2020-03-30	2020-06-28	portalbncochile-cl.xyz	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Subject DN	CN=ayudas-valida-aumento-personas-chile.ml
Issuer DN	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
Serial	293928763198935374154193271638072727304848
Validity	2020-03-30 18:36:13 **to** 2020-06-28 18:36:13 (90 days, 0:00:00)
Names	ayudas-valida-aumento-personas-chile.ml www.ayudas-valida-aumento-personas-chile.ml

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain portalbncochile-cl.xyz 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 ayudas-valida-aumento-personas-chile.ml 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

Location	Russia (RU)
Latitude and Longitude	55.74, 37.61

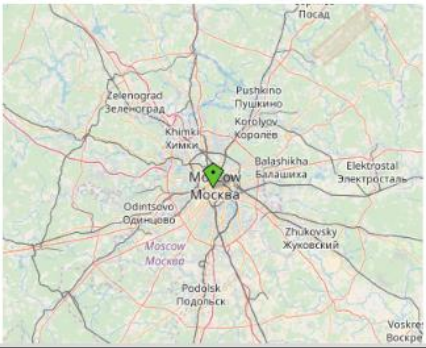
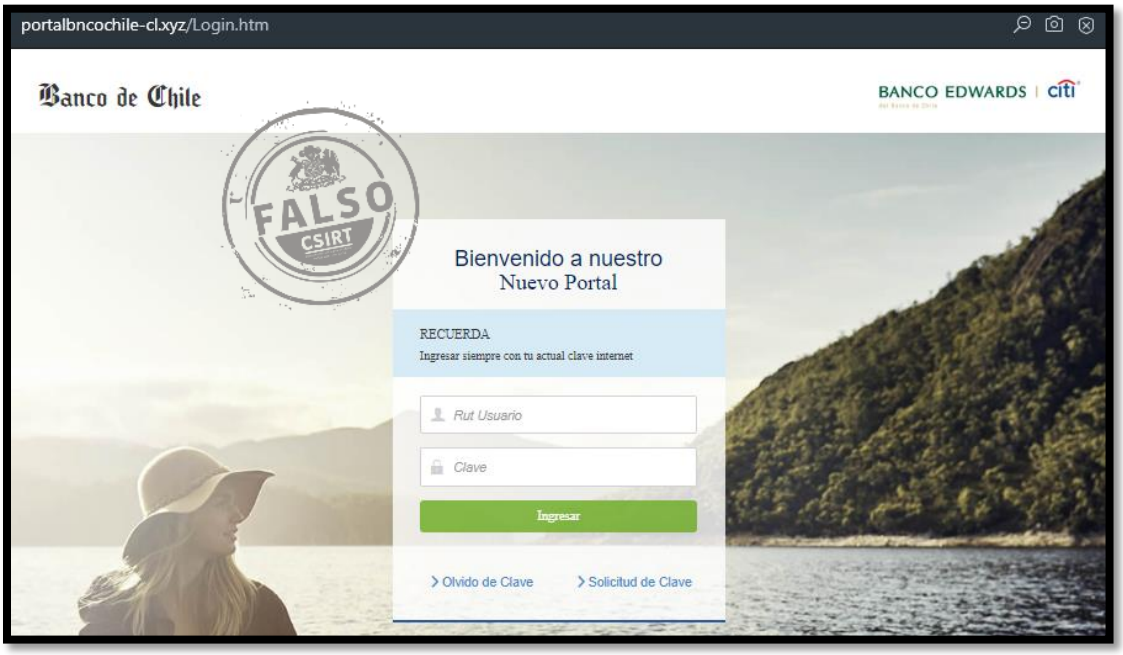
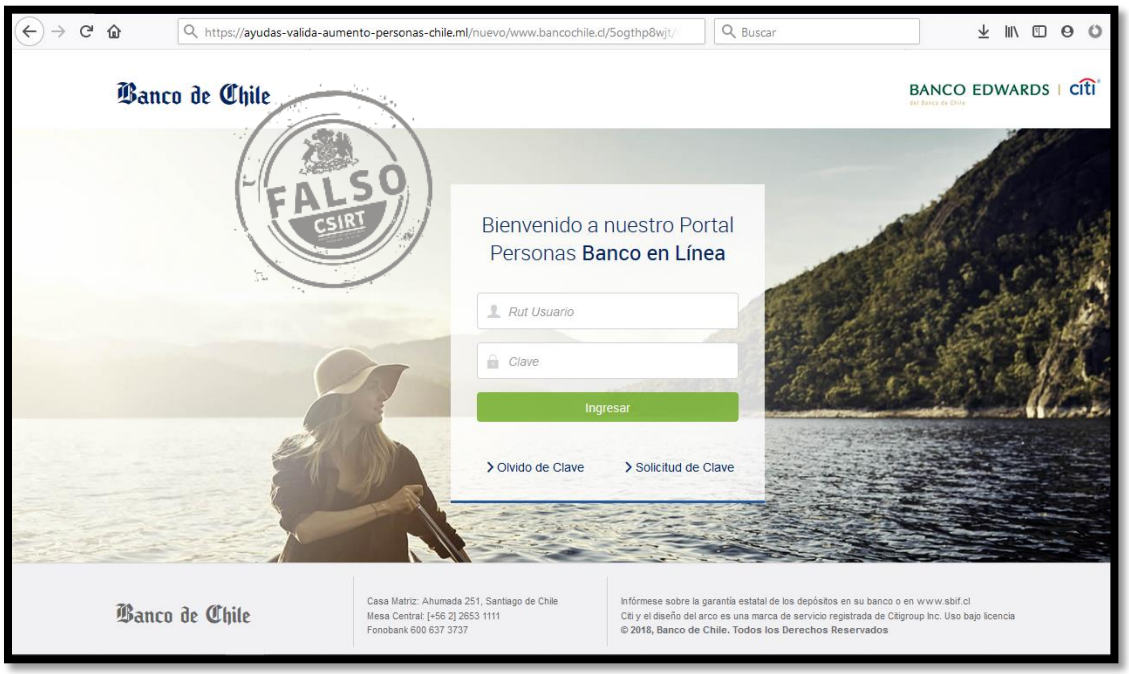


IMAGEN DEL SITIO





WHOIS

```
Domain name: portalbncochile-cl.xyz
Registry Domain ID: D180706094-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-03-30T18:37:28.00Z
Registrar Registration Expiration Date: 2021-03-30T18:37:28.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registry Registrant ID:
Registrant Name: WhoisGuard Protected
Registrant Organization: WhoisGuard, Inc.
Registrant Street: P.O. Box 0823-03411
Registrant City: Panama
Registrant State/Province: Panama
Registrant Postal Code:
Registrant Country: PA
Registrant Phone: +507.8365503
Registrant Phone Ext:
Registrant Fax: +51.17057182
Registrant Fax Ext:
Registrant Email: bf85495b4be84148a6b96c559c964965.protect@whoisguard.com
Registry Admin ID:
Admin Name: WhoisGuard Protected
Admin Organization: WhoisGuard, Inc.
Admin Street: P.O. Box 0823-03411
Admin City: Panama
Admin State/Province: Panama
Admin Postal Code:
Admin Country: PA
Admin Phone: +507.8365503
Admin Phone Ext:
Admin Fax: +51.17057182
Admin Fax Ext:
Admin Email: bf85495b4be84148a6b96c559c964965.protect@whoisguard.com
Registry Tech ID:
Tech Name: WhoisGuard Protected
Tech Organization: WhoisGuard, Inc.
Tech Street: P.O. Box 0823-03411
Tech City: Panama
Tech State/Province: Panama
Tech Postal Code:
Tech Country: PA
Tech Phone: +507.8365503
Tech Phone Ext:
Tech Fax: +51.17057182
Tech Fax Ext:
Tech Email: bf85495b4be84148a6b96c559c964965.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
```

```
Domain name:
   AYUDAS-VALIDA-AUMENTO-PERSONAS-CHILE.ML

Organisation:
   Freedom Registry, Inc.
   2225 East Bayshore Road #290
   Palo Alto CA 94303
   United States
   Phone: +1 650-681-4172
   Fax: +1 650-681-4173

Domain Nameservers:
   NS01.FREENOM.COM
   NS02.FREENOM.COM
   NS03.FREENOM.COM
   NS04.FREENOM.COM

Your selected domain name is a domain name that has been
cancelled, suspended, refused or reserved at the Point ML Registry

It may be available for re-registration at http://www.point.ml

In the interim, the rights for this domain have been automatically
transferred to Freedom Registry, Inc.

Please be advised that the Point ML Registry, Freenom and
Freedom Registry, Inc. cannot be held responsible for any content
that was previously available at this domain name.

Due to restrictions in Point ML 's Privacy Statement personal information
about the previous registrants of the domain name cannot be released
to the general public.

Point ML is proud to work with numerous governmental law enforcement
agencies to stop spam, fraud, phishing attempts, child pornography and
other illicit content on Point ML websites. These agencies may contact the
Point ML Registry directly with any enquiries they may have regarding the
usage of this domain by previous registrants.
```

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.