Alerta de seguridad informática	**8FFR-00070-001**
Clase de alerta	**Fraude**
Tipo de incidente	**Falsificación de Registros o Identidad**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**25 de Septiembre de 2019**
Última revisión	**25 de Septiembre 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 Estado**, 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

http[://]sictsystems[.]com/user/date/imagenes/comun2008/banca-en-linea-personas[.]html
http[://]www.dis4[.]spaintrotter[.]com/bancoestado[.]cl/bancoestado[.]porky/
http[://]www[.]maxmarineegypt[.]com/en/es/bancoestado[.]porky/
https[://]gruporeactiva[.]cl/estado/

IP´s

198[.]58[.]84[.]227

87[.]98[.]231[.]3

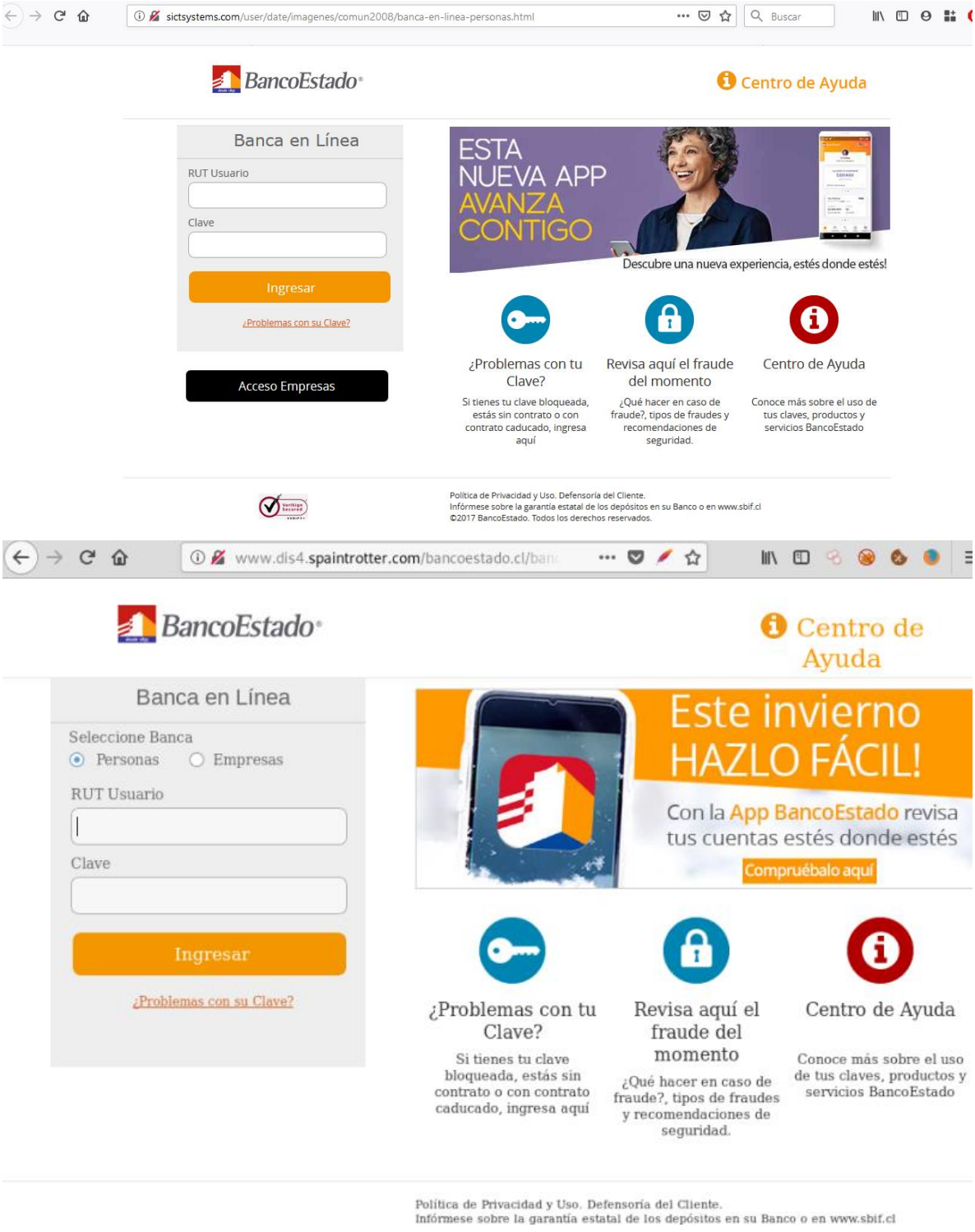
199[.]250[.]196[.]231

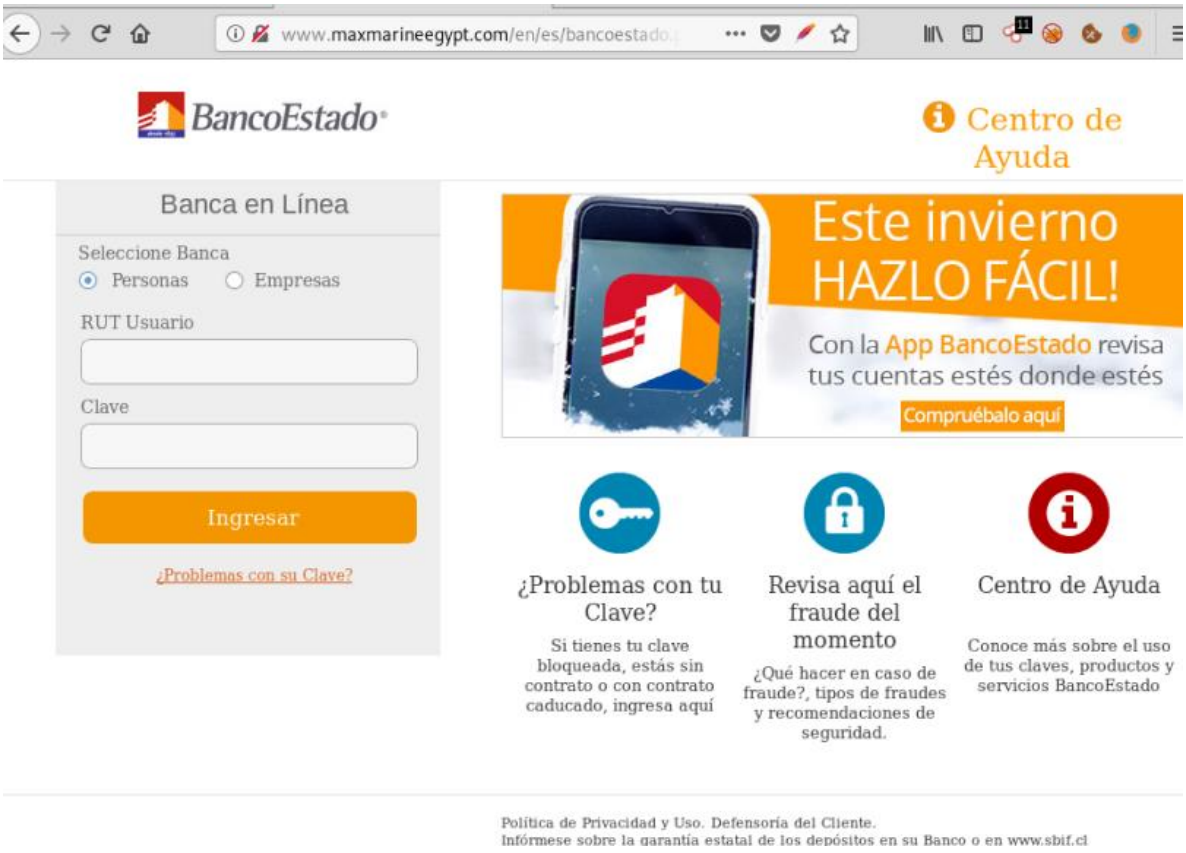
190[.]13[.]188[.]110

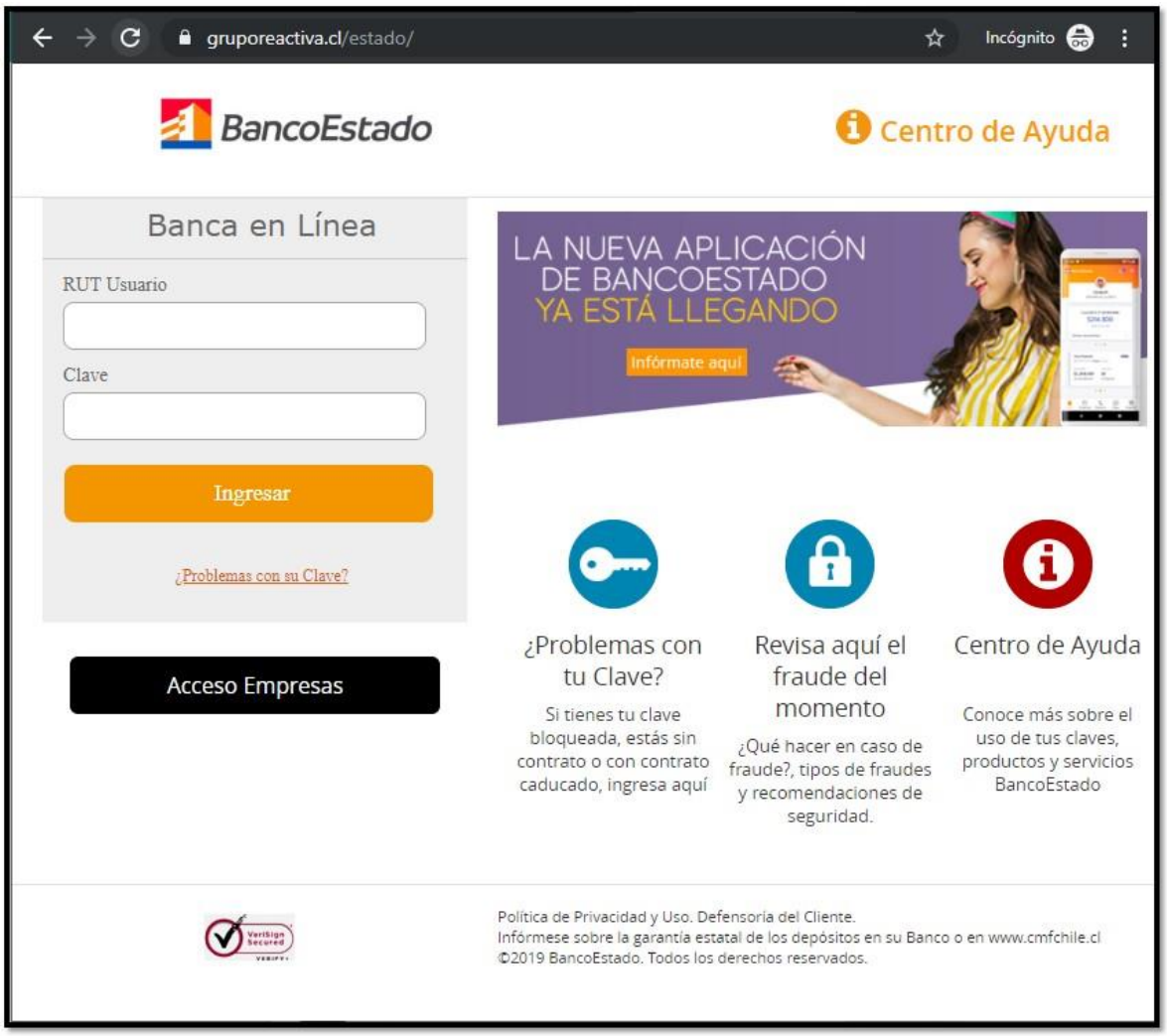
Localización

Austin, Texas, Estados Unidos
Roubaix, Hauts-de-France, Francia
El Segundo, California, Estados Unidos
Valdivia, Los Ríos, Chile

Imagen del sitio




www.maxmarineegypt.com/en/es/bancoestado
BancoEstado
Centro de Ayuda
Banca en Línea
Seleccione Banca
Personas
Empresas
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Este invierno
HAZLO FÁCIL!
Con la App BancoEstado revisa tus cuentas estés donde estés
Compruébalo aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.sbif.cl


gruporeactiva.cl/estado/
Incógnito
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
LA NUEVA APLICACIÓN DE BANCOESTADO YA ESTÁ LLEGANDO
Infórmate aquí
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayuda
Conoce más sobre el uso de tus claves, productos y servicios BancoEstado
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

Whois

```
soc@ITQ-ivps2:~$ whois -h WHOIS.ENOM.COM sictsystems.com


Domain Name: sictsystems.com
Registry Domain ID: 1822889764_DOMAIN_COM-VRSN
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-08-21T05:38:42.00Z
Creation Date: 2013-08-21T20:10:00.00Z
Registrar Registration Expiration Date: 2020-08-21T20:10:28.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registrant Name: Whois Agent (263148063)
Registrant Organization: Whois Privacy Protection Service, Inc.
Registrant Street: PO Box 639
Registrant Street: C/O sictsystems.com
Registrant City: Kirkland
Registrant State/Province: WA
Registrant Postal Code: 98083
Registrant Country: US
Registrant Phone: +1.4252740657
Registrant Phone Ext:
Registrant Fax: +1.4259744730
Registrant Email: wgdptmdkf@whoisprivacyprotect.com
Admin Name: Whois Agent
Admin Organization: Whois Privacy Protection Service, Inc.
Admin Street: PO Box 639
Admin Street: C/O sictsystems.com
Admin City: Kirkland
Admin State/Province: WA
Admin Postal Code: 98083
Admin Country: US
Admin Phone: +1.4252740657
Admin Phone Ext:
Admin Fax: +1.4259744730
Admin Email: wgdptmdkf@whoisprivacyprotect.com
Tech Name: Whois Agent
Tech Organization: Whois Privacy Protection Service, Inc.
Tech Street: PO Box 639
Tech Street: C/O sictsystems.com
Tech City: Kirkland
Tech State/Province: WA
Tech Postal Code: 98083
Tech Country: US
Tech Phone: +1.4252740657
Tech Phone Ext:
Tech Fax: +1.4259744730
Tech Email: wgdptmdkf@whoisprivacyprotect.com
Name Server: YNS1.YAHOO.COM
Name Server: YNS2.YAHOO.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: ABUSE@ENOM.COM
Registrar Abuse Contact Phone: +1.4259744689
URL of the ICANN WHOIS Data Problem Reporting System: HTTP://WDPRS.INTERNIC.NET/
>>> Last update of WHOIS database: 2019-09-24T17:31:25.00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp


The data in this whois database is provided to you for information
purposes only, that is, to assist you in obtaining information about or
related to a domain name registration record. We make this information
```

```
soc@ITQ-ivps2:~$ whois -h whois.ovh.com spaintrotter.com
Domain Name: spaintrotter.com
Registry Domain ID: 1831480009_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.ovh.com
Registrar URL: https://www.ovh.com
Updated Date: 2018-10-12T07:32:39.0Z
Creation Date: 2013-10-17T16:18:41.0Z
Registrar Registration Expiration Date: 2020-10-17T16:18:41.0Z
Registrar: OVH, SAS
Registrar IANA ID: 433
Registrar Abuse Contact Email: abuse@ovh.net
Registrar Abuse Contact Phone: +33.972101007
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization:
Registrant Street:
Registrant City:
Registrant State/Province:
Registrant Postal Code:
Registrant Country: ES
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: 747jj919gimtv0evfavb@z.o-w-o.info
Registry Admin ID:
Admin Name:
Admin Organization:
Admin Street:
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: amxni57483k6nxkwie0i@b.o-w-o.info
Registry Tech ID:
Tech Name:
Tech Organization:
Tech Street:
Tech City:
Tech State/Province:
Tech Postal Code:
Tech Country:
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: amxni57483k6nxkwie0i@b.o-w-o.info
Name Server: dns200.anycast.me
Name Server: ns200.anycast.me
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System:
http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-08-29T23:21:53.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

################################################################################
```

```
soc@ITQ-ivps2:~$ whois -h whois.godaddy.com maxmarineegypt.com
Domain Name: maxmarineegypt.com
Registry Domain ID: 1554787747_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-05-08T10:43:43Z
Creation Date: 2009-05-07T17:51:32Z
Registrar Registration Expiration Date: 2020-05-07T17:51:32Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization: onehoster
Registrant State/Province:
Registrant Country: EG
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=maxma
rineegypt.com
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=maxmarinee
gypt.com
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=maxmarineeg
ypt.com
Name Server: NS1.NEWHOSTERS.COM
Name Server: NS2.NEWHOSTERS.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-09-24T17:00:00Z <<<

For more information on Whois status codes, please visit https://www.icann.org/resources/pages/epp-status-code
s-2014-06-16-en

Notes:

IMPORTANT: Port43 will provide the ICANN-required minimum data set per
ICANN Temporary Specification, adopted 17 May 2018.
Visit https://whois.godaddy.com to look up contact data for domains
not covered by GDPR policy.

The data contained in GoDaddy.com, LLC's WhoIs database,
while believed by the company to be reliable, is provided "as is"
with no guarantee or warranties regarding its accuracy.  This
information is provided for the sole purpose of assisting you
in obtaining information about domain name registration records.
Any use of this data for any other purpose is expressly forbidden without the prior written
permission of GoDaddy.com, LLC.  By submitting an inquiry,
you agree to these terms of usage and limitations of warranty.  In particular,
you agree not to use this data to allow, enable, or otherwise make possible,
dissemination or collection of this data, in part or in its entirety, for any
purpose, such as the transmission of unsolicited advertising and
and solicitations of any kind, including spam.  You further agree
not to use this data to enable high volume, automated or robotic electronic
processes designed to collect or compile this data for any purpose,
including mining this data for your own personal or commercial purposes.

Please note: the registrant of the domain name is specified
in the "registrant" section.  In most cases, GoDaddy.com, LLC
is not the registrant of domain names listed in this database.
soc@ITQ-ivps2:~$
```

```
soc@ITQ-ivps2:~$ whois -h whois.nic.cl gruporeactiva.cl
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: gruporeactiva.cl
Registrant name: TecnologÃ-as y publicidad Escalon limitada
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 2019-04-23 15:04:30 CLST
Expiration date: 2020-04-23 15:04:30 CLST
Name server: ns1.escalon.cl
Name server: ns2.escalon.cl
Name server: ns3.escalon.cl
Name server: ns4.escalon.cl
```

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: 2019.09.25 12:14:03 -03'00'