Alerta de seguridad informática	8FFR-00119-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Noviembre de 2019
Última revisión	22 de Noviembre 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

URL Sitio Clonado:
https[://]bancoestado[.]cl[.]com-cl[.]xyz/imagenes/comun2008/banca-en-linea-personas[.]html
http[://]www[.]winecause[.]com/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

Domain bancoestado.cl.com-cl.xyz

bancoestado / cl / com-cl / xyz / Subdomains

record type	TTL	value	
A	14400	70.32.23.4	

Ilustración 1 Dominio donde se Aloja Url del Banco Estado, Falso y DNS que utiliza

Certificado

Criteria	Identity = 'bancoestado.cl.com-cl.xyz'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
2120264312	2019-11-17	2019-11-16	2020-02-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2120264294	2019-11-17	2019-11-16	2020-02-14	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Criteria	Identity = 'winecause.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Issuer Name
1896201574	2019-09-17	2019-09-17	2019-12-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1896201445	2019-09-17	2019-09-17	2019-12-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1637015969	2019-07-03	2019-07-03	2019-10-01	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1637015982	2019-07-03	2019-07-03	2019-10-01	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1398215587	2019-04-18	2019-04-18	2019-07-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1398212880	2019-04-18	2019-04-18	2019-07-17	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1164917137	2019-02-01	2019-02-01	2019-05-02	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
1164917257	2019-02-01	2019-02-01	2019-05-02	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
954454800	2018-11-17	2018-11-17	2019-02-15	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
954454820	2018-11-17	2018-11-17	2019-02-15	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
714208086	2018-09-02	2018-09-02	2018-12-01	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
714208042	2018-09-02	2018-09-02	2018-12-01	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
535522691	2018-06-18	2018-06-18	2018-09-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
535522392	2018-06-18	2018-06-18	2018-09-16	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
383020774	2018-04-08	2018-04-03	2018-07-02	C=US, ST=TX, L=Houston, O="cPanel, Inc.", CN="cPanel, Inc. Certification Authority"
375669506	2018-04-03	2018-04-03	2018-07-02	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 Estado

IP

70.32.23.4

27.121.67.120

Domain bancoestado.cl.com-cl.xyz is located on IP address << 70.32.23.4 >>

Block start	70.32.16.0
End of block	70.32.31.255
Block size	4096 Domains in block
Block name	ROCKSOLID-NETWORK
AS number	55293
Parent block	70.32.0.0 - 70.32.31.255
Organization	RockSolid Network, Inc.
City	Ann Arbor
Region/State	Michigan
Country	US , United States
Reg. date	2009-01-15
Host name	mi3-ss40.a2hosting.com

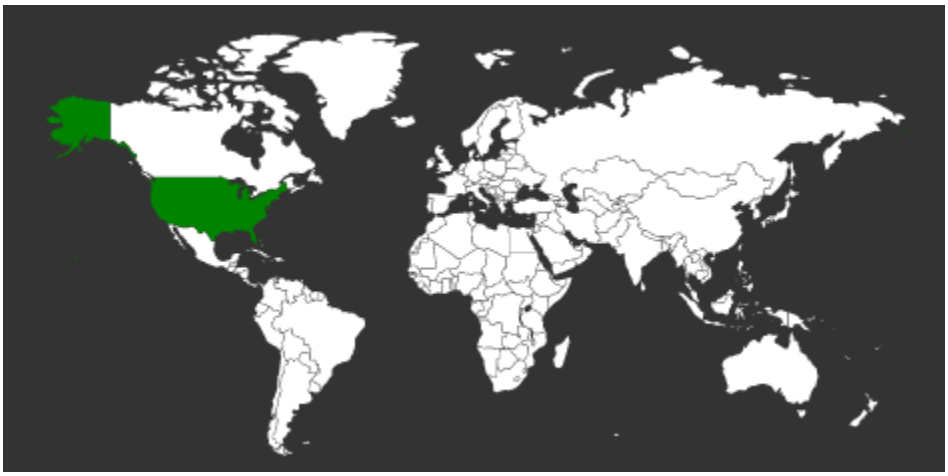
Network information

DNS server (NS records)	ns-1.ezyreg.com (180.235.128.119) ns-2.ezyreg.com (202.191.61.219)
Mail server (MX records)	winecause.com (27.121.67.120)
IP address (IPv4)	27.121.67.120
IP address (IPv6)	
ASN number	24446
ASN name (ISP)	WEBCENTRAL PTY LTD

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

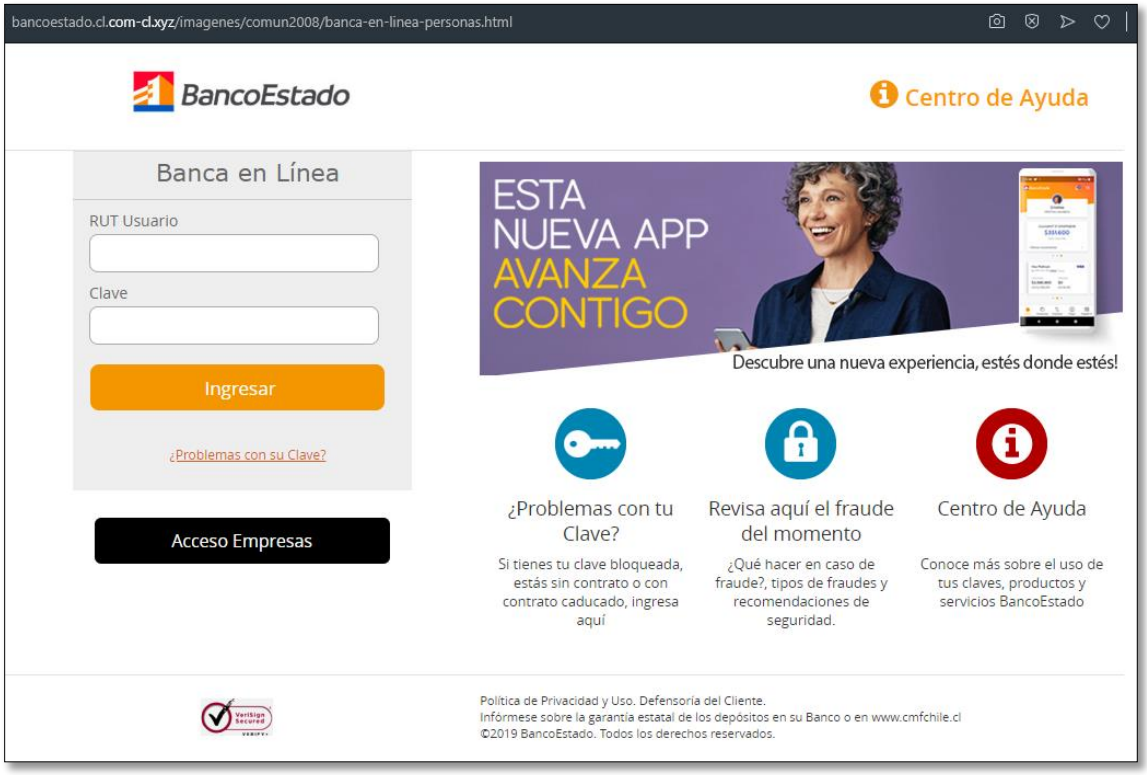
Localización

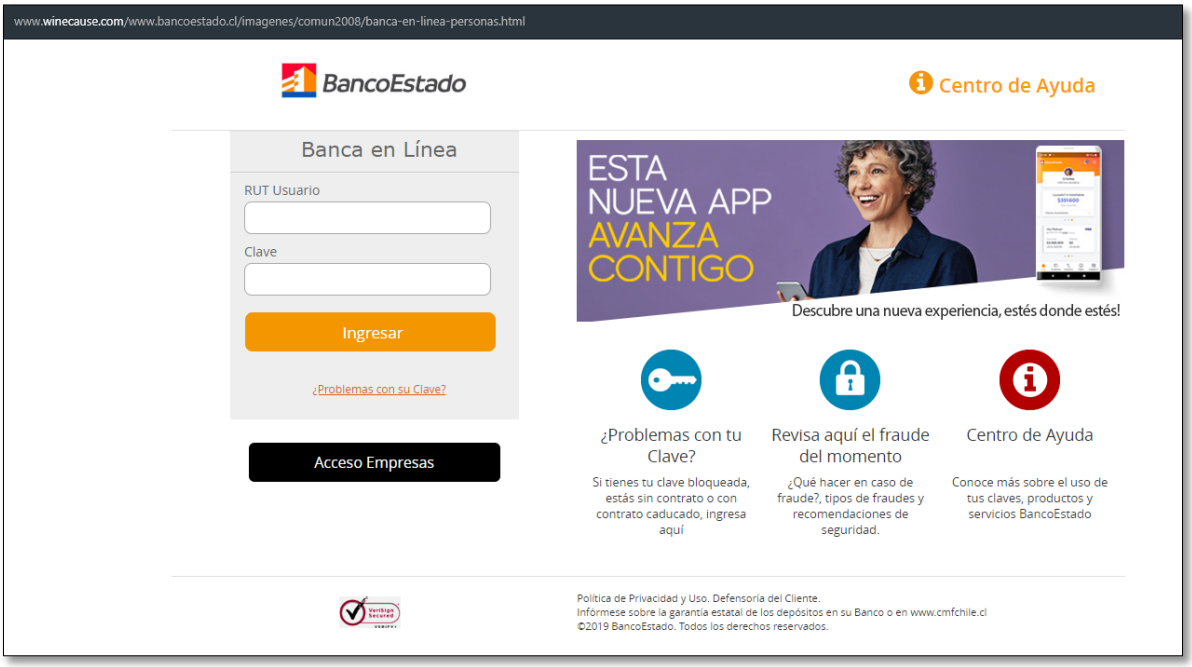
Ann Arbor, Michigan, Estados Unidos



Brisbane, Queensland, Australia

Imagen del sitio





Whois

```
Domain Name: com-cl.xyz
Registry Domain ID: D145602045-CNIC
Registrar WHOIS Server: WHOIS.ENOM.COM
Registrar URL: WWW.ENOM.COM
Updated Date: 2019-11-16T05:14:19.00Z
Creation Date: 2019-11-16T05:14:00.00Z
Registrar Registration Expiration Date: 2020-11-16T05:14:00.00Z
Registrar: ENOM, INC.
Registrar IANA ID: 48
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
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: lima
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: PE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: https://tieredaccess.com/contact/7c506b61-50a9-4ca0-8860-874a63676c65
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.A2HOSTING.COM
Name Server: NS2.A2HOSTING.COM
Name Server: NS3.A2HOSTING.COM
Name Server: NS4.A2HOSTING.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: 2019-11-18T13:40:47.00Z <<<
```

```
Domain Name: winecause.com
Registry Domain ID: 535552257_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.netregistry.com.au
Registrar URL: http://www.netregistry.com.au
Updated Date: 2019-06-27T23:52:44Z
Creation Date: 2006-07-29T02:33:06Z
Registrar Registration Expiration Date: 2020-07-29T02:33:07Z
Registrar: Netregistry Pty Ltd
Registrar IANA ID: 677
Registrar Abuse Contact Email: feedback@netregistry.com.au
Registrar Abuse Contact Phone: +61.299340501
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID:
Registrant Name: Peter Scott
Registrant Organization: PJ & DFS Pty Ltd
Registrant Street: 32 Brisbane Water Road
Registrant City: Adamstown
Registrant State/Province: NSW
Registrant Postal Code: 2289
Registrant Country: AU
Registrant Phone: +61.419227152
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: peter@anotherplanet.com.au
Registry Admin ID:
Admin Name: Peter Scott
Admin Organization: PJ & DFS Pty Ltd
Admin Street: 32 Brisbane Water Road
Admin City: Adamstown
Admin State/Province: NSW
Admin Postal Code: 2289
Admin Country: AU
Admin Phone: +61.419227152
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: peter@anotherplanet.com.au
Registry Tech ID:
Tech Name: Peter Scott
Tech Organization: PJ & DFS Pty Ltd
Tech Street: 32 Brisbane Water Road
Tech City: Adamstown
Tech State/Province: NSW
Tech Postal Code: 2289
Tech Country: AU
Tech Phone: +61.419227152
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: peter@anotherplanet.com.au
Name Server: NS-1.EZYREG.COM
Name Server: NS-2.EZYREG.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2019-11-18T13:50:42Z <<<
```

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: 2019.11.22 20:29:16 -03'00'