| | |
|---|---|
| **Alerta de seguridad informática** | **8FFR-00045-001** |
| **Clase de alerta** | **Fraude** |
| **Tipo de incidente** | **Falsificación de Registros o Identidad** |
| **Nivel de riesgo** | **Alto** |
| **TLP** | **Blanco** |
| **Fecha de lanzamiento original** | **07 de Septiembre de 2019** |
| **Última revisión** | **07 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 del **bancoestado.cl,** 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.

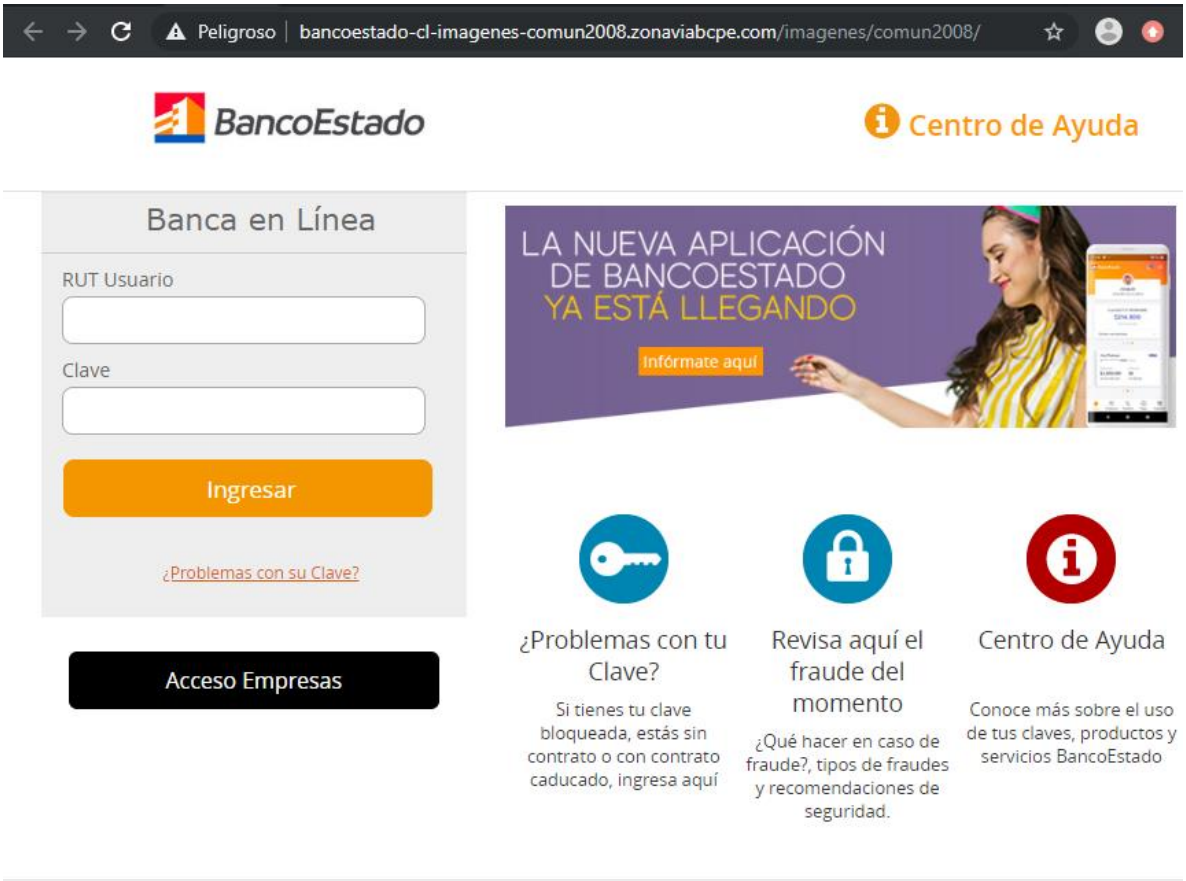
**Indicadores de Compromisos**

**URL´s**
http[://]bancoestado-cl-imagenes-comun2008[.]zonaviabcpe[.]com/imagenes/comun2008/

**IP´s**
158.[.]69[.]243[.]52

**Localización**
Beauharnois, Quebec, Canda

**Ejemplo de Imagen del sitio**



## Whois

```
soc@kali:~$ whois -h whois.psi-usa.info zonaviabcpe.com
Domain Name: zonaviabcpe.com
Registry Domain ID: 2428017611_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.psi-usa.info
Registrar URL: https://www.psi-usa.info
Updated Date: 2019-08-29T16:32:27Z
Creation Date: 2019-08-29T16:32:15Z
Registrar Registration Expiration Date: 2020-08-29T16:32:15Z
Registrar: PSI-USA, Inc. dba Domain Robot
Registrar IANA ID: 151
Registrar Abuse Contact Email: domain-abuse@psi-usa.info
Registrar Abuse Contact Phone: +49.94159559482
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
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: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: https://contact.domain-robot.org/zonaviabcpe.com
Registry Admin ID: REDACTED FOR PRIVACY
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: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: https://contact.domain-robot.org/zonaviabcpe.com
Registry Tech ID: REDACTED FOR PRIVACY
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: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: https://contact.domain-robot.org/zonaviabcpe.com
Name Server: ns35.hosterbox.com
Name Server: ns36.hosterbox.com
DNSSEC: unsigned
```

**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: 2019.09.07
22:19:24 -04'00'