| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00428-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 23 de Mayo de 2020 |
| Última revisión | 23 de Mayo 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 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 compromiso

URL
bancapersonas[.]bancoestado[.]cl[.]arzala[.]com/imagenes/comun2008/banca-en-linea-personas[.]html

IP
199[.]168[.]189[.]50

# Dominios donde se aloja url

**Domain bancapersonas.bancoestado.cl.arzala.com**

bancapersonas / bancoestado / cl / arzala / com / Subdomains

| record type | TTL | value |
|---|---|---|
| A | 14400 | 199.168.189.50 |

**Domain bancoestado.cl.arzala.com**

bancoestado / cl / arzala / com / Subdomains

| record type | TTL | value |
|---|---|---|
| No records found | | |

**Domain arzala.com**

arzala / com / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 14400 | 199.168.189.50 | | |
| NS | 86400 | ns1.pixeldesigncr.com | Zones on DNS server | 199.168.189.50 |
| NS | 86400 | ns2.pixeldesigncr.com | Zones on DNS server | 199.168.189.50 |
| MX | 14400 | 0 arzala.com | | |
| TXT | 14400 | v=spf1 ip4:199.168.189.50 +a +mx ~all | | |

| SOA | 86400 | Mname | ns1.pixeldesigncr.com |
|---|---|---|---|
| | | Rname | soporte.pixelcr.com |
| | | Serial number | 2020051903 |
| | | Refresh | 86400 |
| | | Retry | 7200 |
| | | Expire | 3600000 |
| | | Minimum TTL | 86400 |

# Certificados

## Basic Information

| | |
|---|---|
| **Subject DN** | CN=bancapersonas.bancoestado.cl.arzala.com |
| **Issuer DN** | C=US, ST=TX, L=Houston, O=cPanel, Inc., CN=cPanel, Inc. Certification Authority |
| **Serial** | Decimal: 133462423677408483340305272039499509369<br>Hex: 0x6467ed85aeb27423e09cd770aaea2e79 |
| **Validity** | 2020-05-19 00:00:00 **to** 2020-08-17 23:59:59 (90 days, 23:59:59) |
| **Names** | bancapersonas.bancoestado.cl.arzala.com<br>www.bancapersonas.bancoestado.cl.arzala.com |

# Ip de origen donde se aloja sitio

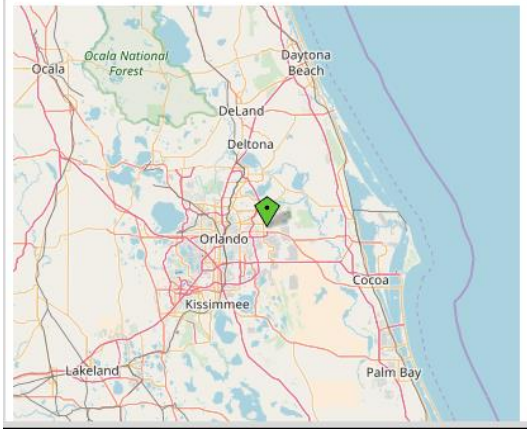
**Domain**
**bancapersonas.bancoestado.cl.arzala.com**
**is located on**
**IP address**
**<< 199.168.189.50 >>**

| | |
|---|---|
| **Block start** | 199.168.184.0 |
| **End of block** | 199.168.191.255 |
| **Block size** | 2048 Domains in block |
| **Block name** | DIMENOC |
| **AS number** | 33182 |
| **Parent block** | 199.0.0.0 - 199.255.255.255 |
| **Organization** | HostDime.com,Inc. |

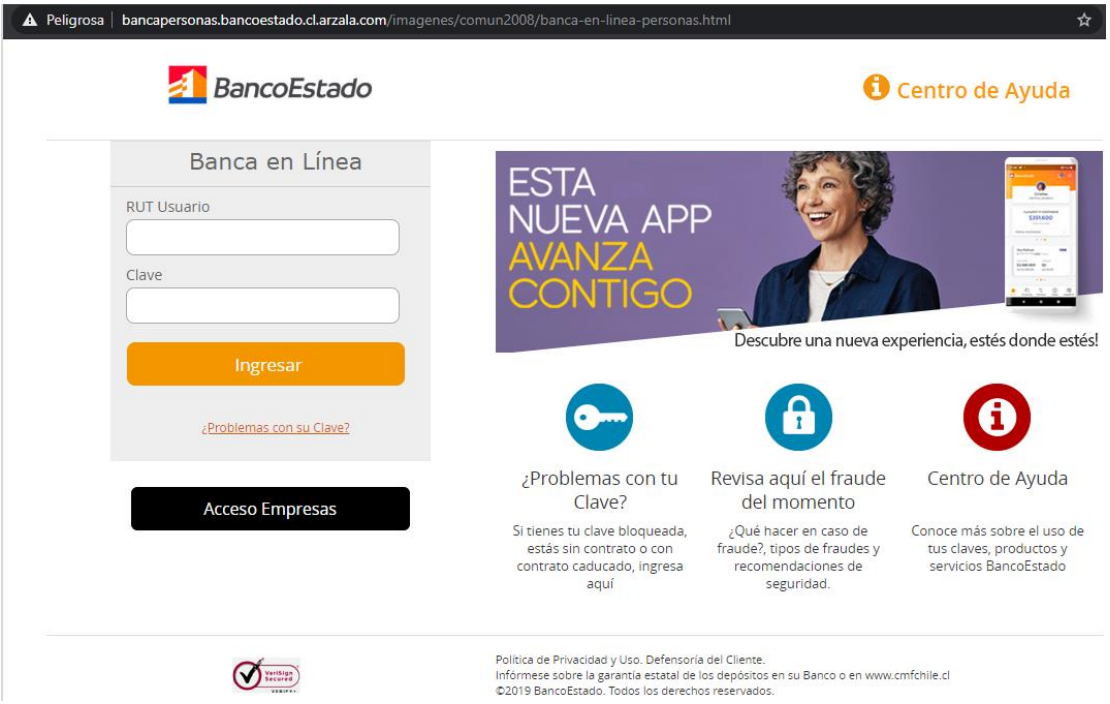
# Localización

Orlando, Florida, Estados unidos

| | |
|---|---|
| Location | Orlando, Florida, United States (US) |
| Latitude and Longitude | 28.58, -81.19 |




# Imagen del sitio



## Whois

```
Domain Name: ARZALA.COM
Registry Domain ID: 548889867_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2019-08-13T21:20:11Z
Creation Date: 2006-08-09T16:50:24Z
Registrar Registration Expiration Date: 2020-08-09T16:50:24Z
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: Pixel Design Costa Rica
Registrant State/Province: San Jose
Registrant Country: CR
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/resul
ts.aspx?domain=ARZALA.COM
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.as
px?domain=ARZALA.COM
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.asp
x?domain=ARZALA.COM
Name Server: NS1.PIXELDESIGNCR.COM
Name Server: NS2.PIXELDESIGNCR.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-05-22T14:00:00Z <<<
```

## 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.