| | |
|---|---|
| Alerta de seguridad cibernética | 8FFR20-00294-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 31 de Marzo de 2020 |
| Última revisión | 31 de Marzo 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), advierte la activación de un portal fraudulento asociado a una IPs 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

bancapersonasbancoestado[.]xyz

www[.]bancapersonasbancoestado[.]xyz

www[.]bancapersonasbancoestado[.]xyz/1585569286/imagenes/comun2008/banca-en-linea-personas[.]html

IP

217[.]182[.]64[.]245

# DOMINIOS DONDE SE ALOJA URL

**Domain bancapersonasbancoestado.xyz**

bancapersonasbancoestado / xyz / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 1799 | 217.182.64.245 | | |
| 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 | 1585548948 |
| Refresh | 43200 |
| Retry | 3600 |
| Expire | 604800 |
| Minimum TTL | 3601 |

# CERTIFICADOS

Certificates

| crt.sh ID | Logged At | Not Before | Not After | Matching Identities | Issuer Name |
|---|---|---|---|---|---|
| 2644373150 | 2020-03-30 | 2020-03-30 | 2020-06-28 | bancapersonasbancoestado.xyz<br>www.bancapersonasbancoestado.xyz | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 2644507327 | 2020-03-30 | 2020-03-30 | 2020-06-28 | bancapersonasbancoestado.xyz<br>www.bancapersonasbancoestado.xyz | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |

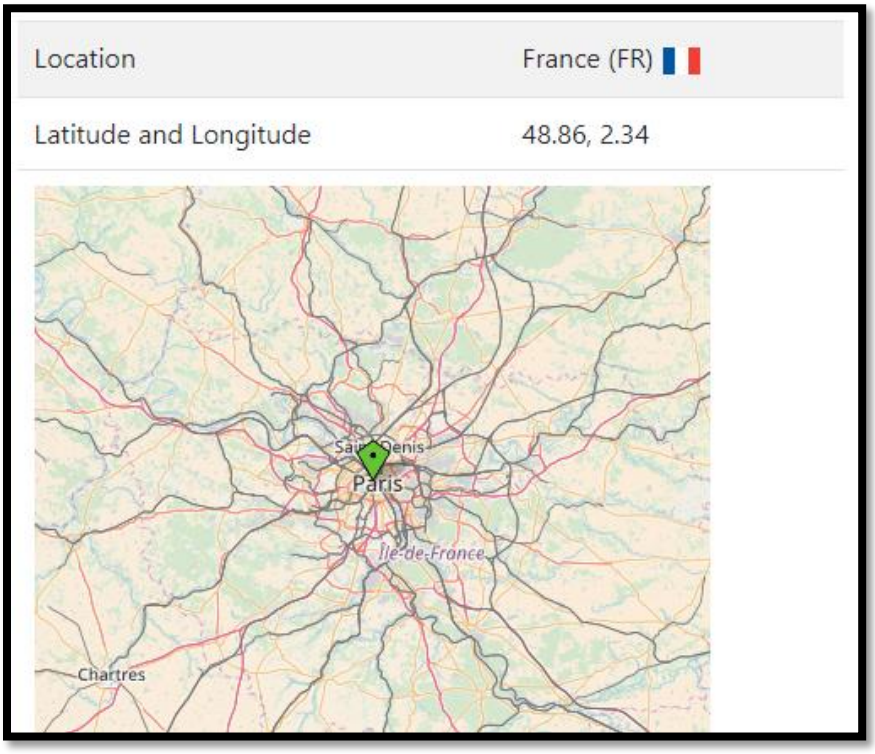
# IP DE ORIGEN DONDE SE ALOJA SITIO

**Domain bancapersonasbancoestado.xyz is located on IP address << 217.182.64.245 >>**

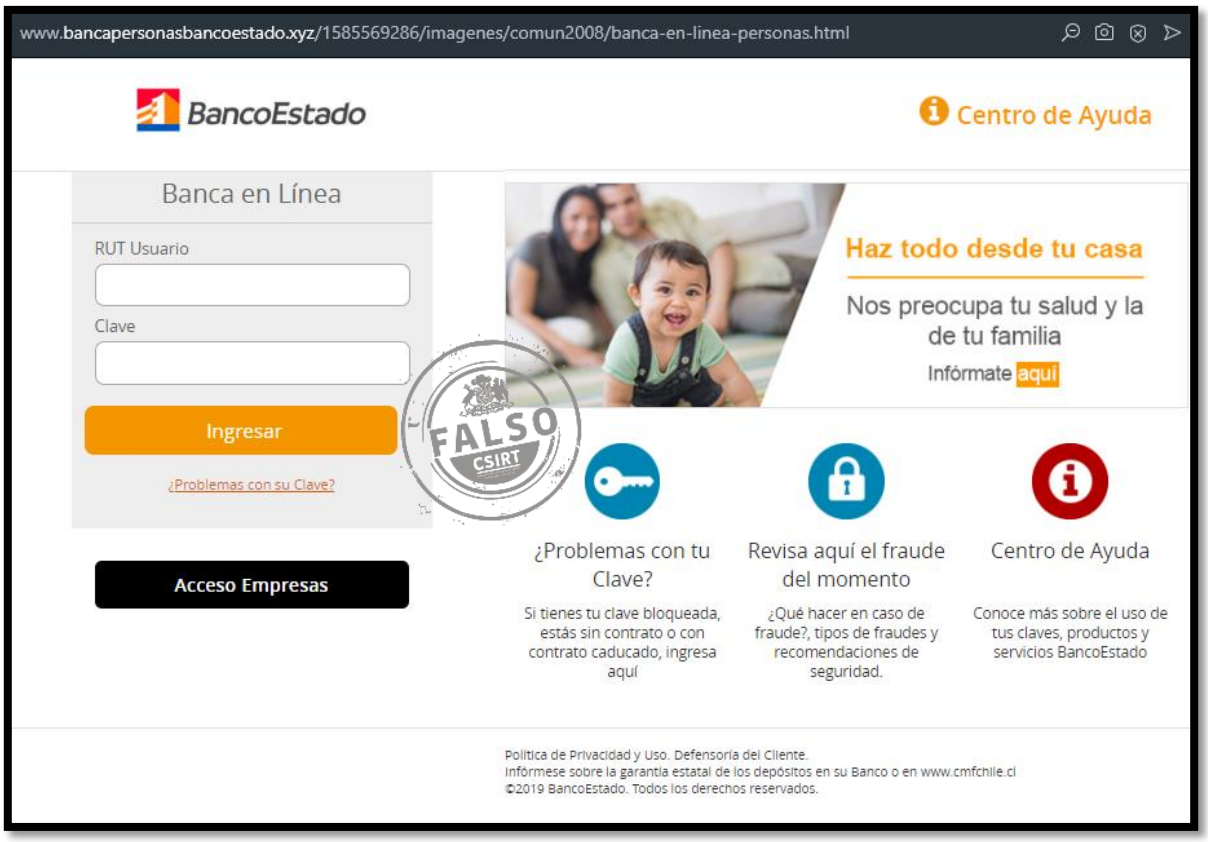
| | |
|---|---|
| **Block start** | 217.182.0.0 |
| **End of block** | 217.182.255.255 |
| **Block size** | 65536 Domains in block |
| **Block name** | FR-OVH-20010302 |
| **AS number** | 16276 |
| **Parent block** | 217.0.0.0 - 217.255.255.255 |
| **Organization** | ORG-OS3-RIPE |

# LOCALIZACIÓN

Francia



# IMAGEN DEL SITIO



# WHOIS

```
Domain name: bancapersonasbancoestado.xyz
Registry Domain ID: D180614294-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2020-03-30T06:01:59.00Z
Registrar Registration Expiration Date: 2021-03-30T06:01:59.00Z
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: c0546b0470ac430e9e51c5534b821feb.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: c0546b0470ac430e9e51c5534b821feb.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: c0546b0470ac430e9e51c5534b821feb.protect@whoisguard.com
Name Server: dns1.registrar-servers.com
Name Server: dns2.registrar-servers.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-03-30T04:12:34.02Z <<<
```

# 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: 2020.03.31 09:21:29 -03'00'