| | |
|---|---|
| **Alerta de seguridad informática** | **8FFR-00100-001** |
| **Clase de alerta** | **Fraude** |
| **Tipo de incidente** | **Falsificación de Registros o Identidad** |
| **Nivel de riesgo** | **Alto** |
| **TLP** | **Blanco** |
| **Fecha de lanzamiento original** | **28 de Octubre de 2019** |
| **Última revisión** | **28 de Octubre 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[://]bancorestado[.]website/imagenes/empresas2008/Acceso_empresas/acceso_clientes[.]html

https[://]bancoestaado[.]xyz/imagenes/comun2009/en-linea-personas[.]php

http[://]bancoesstado[.]xyz/imagenes/comun2009/en-linea-personas[.]php

**Domain bancorestado.website**

bancorestado / website / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 1200 | 199.188.206.58 | | |
| NS | 1800000 | dns1.namecheaphosting.com | Zones on DNS server | 216.87.155.33 |
| NS | 1800000 | dns2.namecheaphosting.com | Zones on DNS server | 216.87.152.33 |
| MX | 1200 | 0 mail.bancorestado.website | | |

| SOA | 1800000 | | |
|---|---|---|---|
| | | Mname | dns1.namecheaphosting.com |
| | | Rname | cpanel.tech.namecheap.com |
| | | Serial number | 2019102802 |
| | | Refresh | 86400 |
| | | Retry | 7200 |
| | | Expire | 3600000 |
| | | Minimum TTL | 86400 |

**Domain bancoestaado.xyz**

bancoestaado / xyz / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 7207 | 139.59.74.245 | | |
| NS | 172800 | ns1.dnsowl.com | Zones on DNS server | 198.251.84.16, 104.207.141.138, 185.34.216.159 |
| NS | 172800 | ns2.dnsowl.com | Zones on DNS server | 168.235.75.52, 64.32.22.100, 45.32.237.128 |
| NS | 172800 | ns3.dnsowl.com | Zones on DNS server | 209.141.39.150, 45.63.5.234, 45.63.106.63 |

| SOA | 172800 | | |
|---|---|---|---|
| | | Mname | ns1.dnsowl.com |
| | | Rname | hostmaster.dnsowl.com |
| | | Serial number | 1572271191 |
| | | Refresh | 7200 |
| | | Retry | 1800 |
| | | Expire | 1209600 |
| | | Minimum TTL | 600 |

**Domain bancoesstado.xyz**

bancoesstado / xyz / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 7207 | 139.59.67.15 | | |
| NS | 172800 | ns1.dnsowl.com | Zones on DNS server | 198.251.84.16, 104.207.141.138, 185.34.216.159 |
| NS | 172800 | ns2.dnsowl.com | Zones on DNS server | 45.32.237.128, 168.235.75.52, 64.32.22.100 |
| NS | 172800 | ns3.dnsowl.com | Zones on DNS server | 45.63.106.63, 209.141.39.150, 45.63.5.234 |
| SOA | 172800 | Mname | ns1.dnsowl.com | |
| | | Rname | hostmaster.dnsowl.com | |
| | | Serial number | 1572270600 | |
| | | Refresh | 7200 | |
| | | Retry | 1800 | |
| | | Expire | 1209600 | |
| | | Minimum TTL | 600 | |

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

**Certificado**

*Ilustración 2 Certificado Utilizado en Url del sitio Falso del Banco Estado*

**IP´s**

199[.]188[.]206[.]58

139[.]59[.]74[.]245

139[.]59[.]67[.]15

**Domain bancorestado.website is located on IP address << 199.188.206.58 >>**

| | |
|---|---|
| Block start | 199.188.200.0 |
| End of block | 199.188.207.255 |
| Block size | 2048 Domains in block |
| Block name | NCNET-1 |
| AS number | 22612 |
| Parent block | 199.0.0.0 - 199.255.255.255 |
| Organization | Namecheap, Inc. |
| City | Atlanta |
| Region/State | Georgia |
| Country | US , United States |
| Reg. date | 2011-08-03 |
| Host name | cavooit.com |
| Web server | Apache |

| Domain bancoestaado.xyz is located on IP address << 139.59.74.245 >> | |
|---|---|
| **Block start** | 139.59.0.0 |
| **End of block** | 139.59.255.254 |
| **Block size** | 65535 Domains in block |
| **Block name** | DIGITALOCEAN-AP |
| **AS number** | 14061 |
| **Parent block** | 139.59.0.0 - 139.59.255.255 |
| **Organization** | DigitalOcean, LLC |
| **Country** | SG , Singapore |
| **Host name** | no record in reverse zone |
| **Domains** | 1 bancoestaado.xyz |

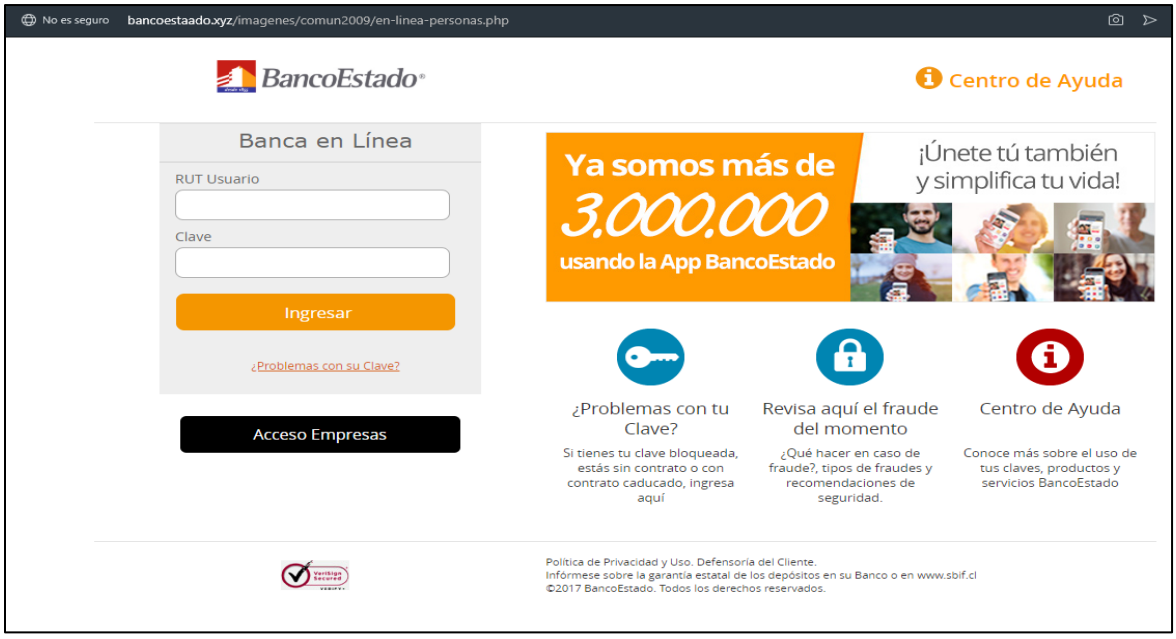
| Domain bancoesstado.xyz is located on IP address << 139.59.67.15 >> | |
|---|---|
| **Block start** | 139.59.0.0 |
| **End of block** | 139.59.255.254 |
| **Block size** | 65535 Domains in block |
| **Block name** | DIGITALOCEAN-AP |
| **AS number** | 14061 |
| **Parent block** | 139.59.0.0 - 139.59.255.255 |
| **Organization** | DigitalOcean, LLC |
| **Country** | SG , Singapore |
| **Host name** | no record in reverse zone |
| **Domains** | 1 bancoesstado.xyz |

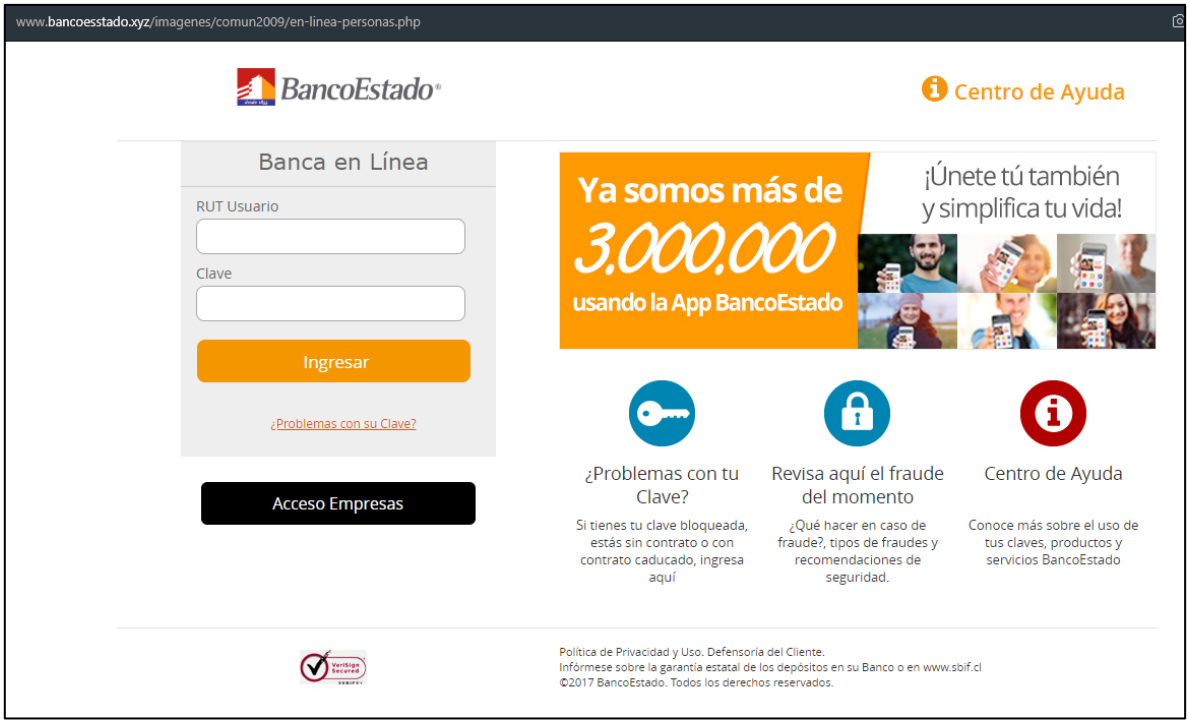
*Ilustración 3 Ip de Origen donde se aloja Sitio Falso del Banco Estado*

**Localización**

Atlanta, Georgia, Estados Unidos
Bangalore, Karnataka, India

**Imagen del sitio**


No es seguro
bancoestaado.xyz/imagenes/comun2009/en-linea-personas.php
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Ya somos más de
3.000.000
usando la App BancoEstado
¡Únete tú también
y simplifica tu vida!
¿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
©2017 BancoEstado. Todos los derechos reservados.


www.bancoesstado.xyz/imagenes/comun2009/en-linea-personas.php
BancoEstado
Centro de Ayuda
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
Ya somos más de
3.000.000
usando la App BancoEstado
¡Únete tú también
y simplifica tu vida!
¿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
©2017 BancoEstado. Todos los derechos reservados.

**Whois**

```
Domain name: bancorestado.website
Registry Domain ID: D137754215-CNIC
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2019-10-28T03:36:29.00Z
Registrar Registration Expiration Date: 2020-10-28T03:36:29.00Z
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: 16a9619d398b42fc993832d40ca7f9b2.protect@whoisguard.com
Name Server: dns1.namecheaphosting.com
Name Server: dns2.namecheaphosting.com
DNSSEC: unsigned
```

```
Domain Name: bancoestaado.xyz
Registry Domain ID: D137640225-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-27T07:00:00Z
Creation Date: 2019-10-27T07:00:00Z
Registrar Registration Expiration Date: 2020-10-27T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-58e6f75883ffa419907ed697d6aebfb7@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-58e6f75883ffa419907ed697d6aebfb7@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-58e6f75883ffa419907ed697d6aebfb7@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
Domain Name: bancoesstado.xyz
Registry Domain ID: D137629135-CNIC
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-27T07:00:00Z
Creation Date: 2019-10-26T07:00:00Z
Registrar Registration Expiration Date: 2020-10-27T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-43792ff51celaa118230028ad525ef2f@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-43792ff51celaa118230028ad525ef2f@privacyguardian.org
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-43792ff51celaa118230028ad525ef2f@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.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: 2019.10.28 15:49:27 -03'00'