| | |
|---|---|
| Alerta de seguridad informática | 8FFR20-00200-01 |
| Clase de alerta | Fraude |
| Tipo de incidente | Falsificación de Registros o Identidad |
| Nivel de riesgo | Alto |
| TLP | Blanco |
| Fecha de lanzamiento original | 30 de Enero de 2020 |
| Última revisión | 30 de Enero 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 cuatro portales fraudulentos asociados a dos IPs que suplantan 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

www1[.]bankestado[.]cl[.]taldo[.]info
www1[.]bankestado[.]cl[.]taldo[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html
www1[.]bankestado[.]cl[.]tadi0[.]info
www1[.]bankestado[.]cl[.]tadi0[.]info/imagenes/comun2008/banca-en-linea-personas[.]php?html

**Domain taldo.info**

taldo / info / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 7207 | 68.183.85.198 | | |
| NS | 172800 | ns1.dnsowl.com | Zones on DNS server | 104.207.141.138, 185.34.216.159, 198.251.84.16 |
| 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 | 45.63.5.234, 209.141.39.150, 45.63.106.63 |
| SOA | 172800 | Mname | ns1.dnsowl.com | |
| | | Rname | hostmaster.dnsowl.com | |
| | | Serial number | 1580310379 | |
| | | Refresh | 7200 | |
| | | Retry | 1800 | |
| | | Expire | 1209600 | |
| | | Minimum TTL | 600 | |

**Domain tadi0.info**

tadi0 / info / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 7207 | 139.59.78.109 | | |
| NS | 172800 | ns1.dnsowl.com | Zones on DNS server | 104.207.141.138, 185.34.216.159, 198.251.84.16 |
| NS | 172800 | ns2.dnsowl.com | Zones on DNS server | 45.32.237.128, 64.32.22.100, 168.235.75.52 |
| 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 | 1580310379 | |
| | | Refresh | 7200 | |
| | | Retry | 1800 | |
| | | Expire | 1209600 | |
| | | Minimum TTL | 600 | |

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

Certificados

| | |
|---|---|
| **Subject DN** | CN=www1.bankestado.cl.taldo.info |
| **Issuer DN** | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| **Serial** | 293864601295179472689126538196952391471517 |
| **Validity** | 2020-01-28 21:22:48 **to** 2020-04-27 21:22:48 (90 days, 0:00:00) |
| **Names** | www1.bankestado.cl.taldo.info |

| | |
|---|---|
| **Subject DN** | CN=www1.bankestado.cl.tadi0.info |
| **Issuer DN** | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| **Serial** | 293462827464272940579425466007357435329657 |
| **Validity** | 2020-01-29 11:47:40 **to** 2020-04-28 11:47:40 (90 days, 0:00:00) |
| **Names** | www1.bankestado.cl.tadi0.info |

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

IP

68[.]183[.]85[.]198

139[.]59[.]78[.]109

**Domain www1.bankestado.cl.taldo.info is located on IP address << 68.183.85.198 >>**

| | |
|---|---|
| **Block start** | 68.183.0.0 |
| **End of block** | 68.183.255.255 |
| **Block size** | 65536 Domains in block |
| **Block name** | DSLEXTREME-NWK-6 |
| **AS number** | 14061 |
| **Parent block** | 68.0.0.0 - 68.255.255.255 |
| **Organization** | DSL Extreme |
| **City** | Chatsworth |
| **Region/State** | California |
| **Country** | US , United States |
| **Reg. date** | 2005-04-14 |
| **Host name** | no record in reverse zone |

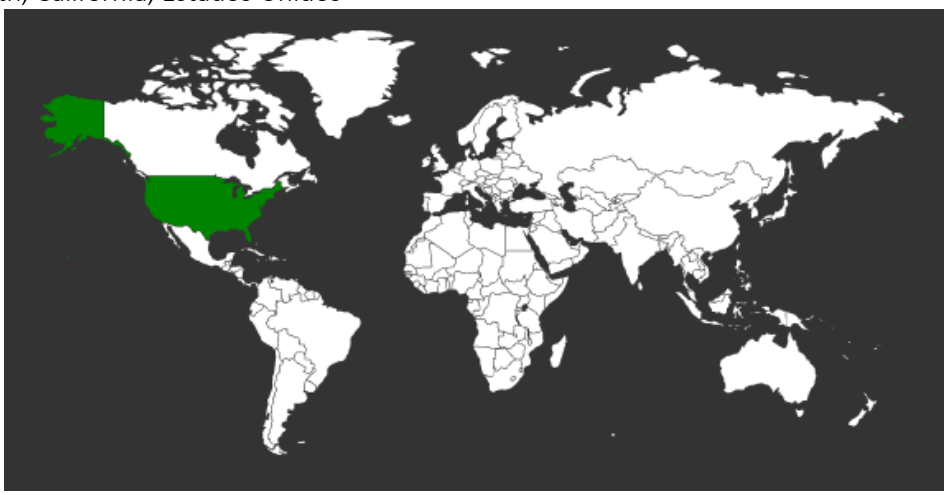
**Domain www1.bankestado.cl.tadi0.info is located on IP address << 139.59.78.109 >>**

| | |
|---|---|
| **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 www1.bankestado.cl.tadi0.info |

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

Localización

Chatsworth, California, Estados Unidos



Singapur, Singapur

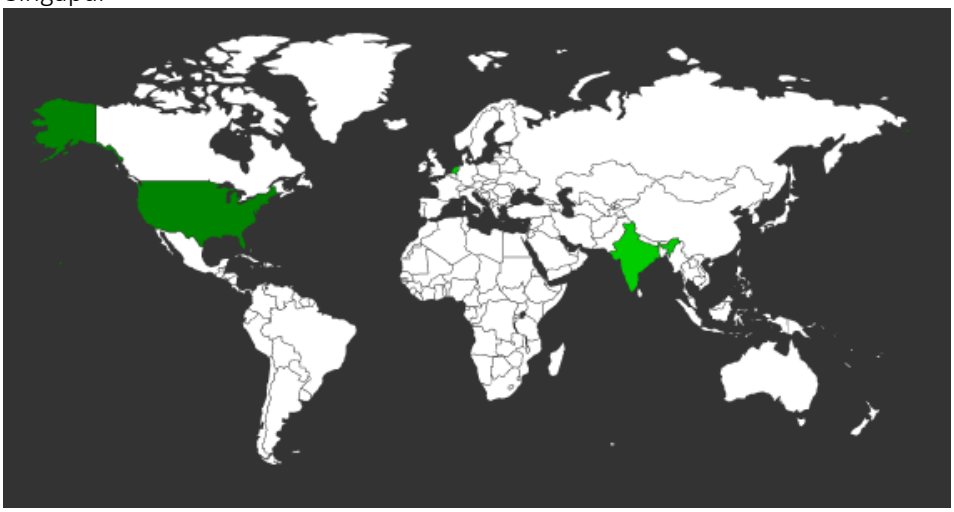
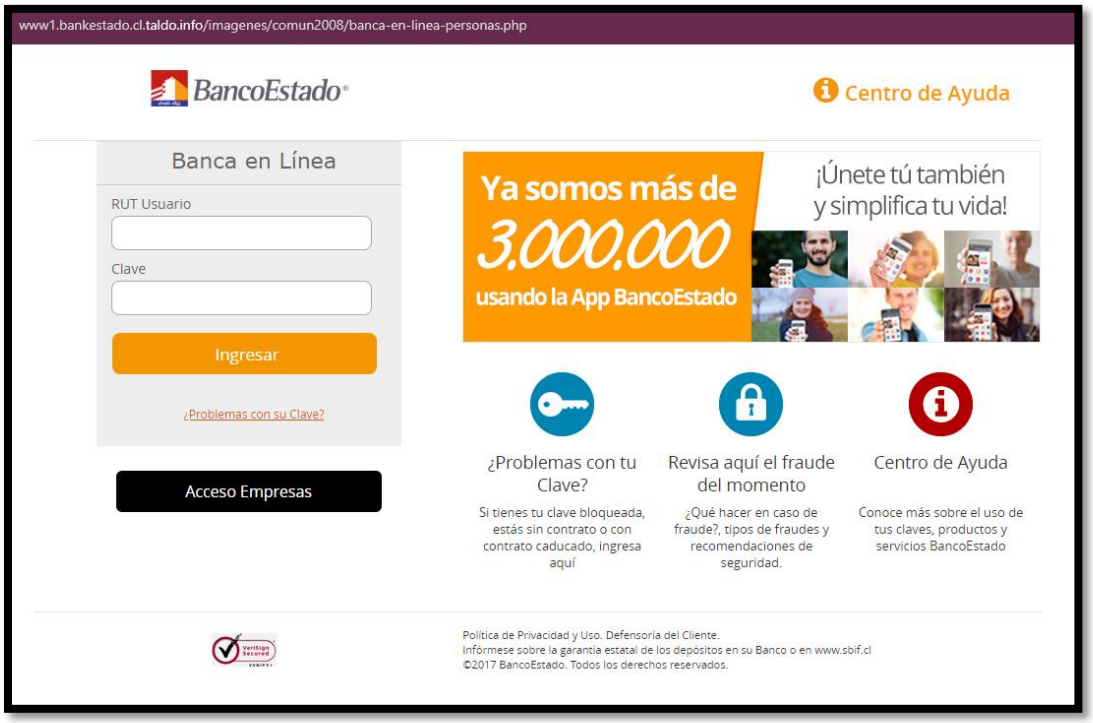


Imagen del sitio




Whois

```
Domain Name: tadi0.info
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-01-29T07:00:00Z
Creation Date: 2020-01-28T07:00:00Z
Registrar Registration Expiration Date: 2021-01-28T07:00:00Z
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-68b67f3121287d8119bd9064dd9fea5c@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-68b67f3121287d8119bd9064dd9fea5c@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-68b67f3121287d8119bd9064dd9fea5c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-01-29T07:00:00Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

```
Domain Name: taldo.info
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-01-29T07:00:00Z
Creation Date: 2020-01-28T07:00:00Z
Registrar Registration Expiration Date: 2021-01-28T07:00:00Z
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-44cf976353e95a0dac5c248baf41c84e@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-44cf976353e95a0dac5c248baf41c84e@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-44cf976353e95a0dac5c248baf41c84e@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-01-29T07:00:00Z <<<
```

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.30 12:57:57 -03'00'