| | |
|---|---|
| **Alerta de seguridad informática** | **8FFR-00094-001** |
| **Clase de alerta** | **Fraude** |
| **Tipo de incidente** | **Falsificación de Registros o Identidad** |
| **Nivel de riesgo** | **Alto** |
| **TLP** | **Blanco** |
| **Fecha de lanzamiento original** | **17 de Octubre de 2019** |
| **Última revisión** | **17 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**

https[://]estado-revision[.]000webhostapp[.]com/

https[://]estado-revision[.]000webhostapp[.]com/imagenes/comun2008/banca-en-linea-personas[.]html
https[://]www[.]bancooestadocl[.]xyz

https[://]www[.]bancooestadocl[.]xyz/imagenes/comun2009/en-linea-personas[.]php
http[://]ironicindia[.]com/warra/imagenes/comun2008/banca-en-linea-personas[.]html

**Domain 000webhostapp.com**

000webhostapp / com / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 60 | 153.92.0.100 | | |
| NS | 900 | dns1.000webhost.com | Zones on DNS server | 153.92.2.10 |
| NS | 900 | dns2.000webhost.com | Zones on DNS server | 153.92.2.20 |
| MX | 3600 | 1 ASPMX.L.GOOGLE.com | | |
| TXT | 3600 | h0xkmxkckcltwjb7v25vhl8c4xngkmst | | |
| TXT | 3600 | google-site-verification=o8fiVtoqn6Pt0erlqmBsJ0dDG0-k7szm03Q3-I_nZ10 | | |

| SOA | 900 | Mname | dns1.000webhost.com |
|---|---|---|---|
| | | Rname | hostmaster.000webhost.com |
| | | Serial number | 1 |
| | | Refresh | 7200 |
| | | Retry | 900 |
| | | Expire | 1209600 |
| | | Minimum TTL | 86400 |

**Domain bancooestadocl.xyz**

bancooestadocl / xyz / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 7207 | 139.59.37.239 | | |
| NS | 172800 | ns1.dnsowl.com | Zones on DNS server | 198.251.84.16, 185.34.216.159, 104.207.141.138 |
| 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 | 209.141.39.150, 45.63.5.234, 45.63.106.63 |

| SOA | 172800 | Mname | ns1.dnsowl.com |
|---|---|---|---|
| | | Rname | hostmaster.dnsowl.com |
| | | Serial number | 1571170806 |
| | | Refresh | 7200 |
| | | Retry | 1800 |
| | | Expire | 1209600 |
| | | Minimum TTL | 600 |

**Domain ironicindia.com**

ironicindia / com / Subdomains

| record type | TTL | value | | |
|---|---|---|---|---|
| A | 14400 | 108.167.146.109 | | |
| NS | 86400 | cns33.webhostbox.net | Zones on DNS server | 108.167.146.106 |
| NS | 86400 | cns34.webhostbox.net | Zones on DNS server | 108.167.146.107 |
| MX | 14400 | 0 mail.ironicindia.com | | |
| TXT | 14400 | v=spf1 +a +mx +ip4:108.167.146.103 ~all | | |
| SOA | 86400 | | | |

| | |
|---|---|
| Mname | cns33.webhostbox.net |
| Rname | root.cs17.webhostbox.net |
| Serial number | 2019092505 |
| Refresh | 86400 |
| Retry | 7200 |
| Expire | 3600000 |
| Minimum TTL | 86400 |

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

## Certificado

Criteria: Identity = '000webhostapp.com'

Certificates

| crt.sh ID | Logged At | Not Before | Not After | Issuer Name |
|---|---|---|---|---|
| 1573772898 | 2019-06-13 | 2019-06-11 | 2021-07-10 | C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018 |
| 1566039480 | 2019-06-11 | 2019-06-11 | 2021-07-10 | C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL RSA CA 2018 |
| 527688102 | 2018-06-15 | 2018-06-13 | 2019-06-13 | C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1 |
| 523435609 | 2018-06-13 | 2018-06-13 | 2019-06-13 | C=US, O=DigiCert Inc, OU=www.digicert.com, CN=RapidSSL TLS RSA CA G1 |
| 21544779 | 2016-06-09 | 2016-06-02 | 2019-06-02 | C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO RSA Domain Validation Secure Server CA |

Criteria: Identity = 'www.bancooestadocl.xyz'

Certificates

| crt.sh ID | Logged At | Not Before | Not After | Issuer Name |
|---|---|---|---|---|
| 2002666622 | 2019-10-15 | 2019-10-15 | 2020-01-13 | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 2002616734 | 2019-10-15 | 2019-10-15 | 2020-01-13 | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |

Criteria: Identity = 'ironicindia.com'

Certificates

| crt.sh ID | Logged At | Not Before | Not After | Issuer Name |
|---|---|---|---|---|
| 1957108864 | 2019-09-25 | 2019-09-25 | 2019-12-24 | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |
| 1926761198 | 2019-09-25 | 2019-09-25 | 2019-12-24 | C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3 |

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

**IP´s**

153[.]92[.]0[.]100

139[.]59[.]37[.]239

108[.]167[.]146[.]109

| Domain 000webhostapp.com is located on IP address << 153.92.0.100 >> | |
|---|---|
| Block start | 153.92.0.0 |
| End of block | 153.92.15.255 |
| Block size | 4096 Domains in block |
| Block name | HOSTINGER-HOSTING |
| AS number | 204915 |
| Parent block | 153.0.0.0 - 153.255.255.255 |
| Organization | ORG-ARTA1-RIPE |
| City | Ashburn |
| Region/State | Virginia |
| Country | US , United States |
| Reg. date | 1991-09-23 |
| Host name | no record in reverse zone |
| Domain count | >= 3 Servers around |
| Domains | 1 000webhostapp.com<br>2 ccshop.comyr.com<br>3 testing112.comuf.com |

| Domain bancooestadocl.xyz is located on IP address << 139.59.37.239 >> | |
|---|---|
| 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 bancooestadocl.xyz |

| Domain ironicindia.com is located on IP address << 108.167.146.109 >> | |
|---|---|
| **Block start** | 108.167.128.0 |
| **End of block** | 108.167.191.255 |
| **Block size** | 16384 Domains in block |
| **Block name** | HGBLOCK-4 |
| **AS number** | 46606 |
| **Parent block** | 108.0.0.0 - 108.255.255.255 |
| **Organization** | WEBSITEWELCOME.COM |
| **City** | Houston |
| **Region/State** | Texas |
| **Country** | US , United States |
| **Reg. date** | 2011-12-27 |
| **Host name** | no record in reverse zone |

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

**Localización**

Virginia, EEUU

Texas, EEUU

Singapur

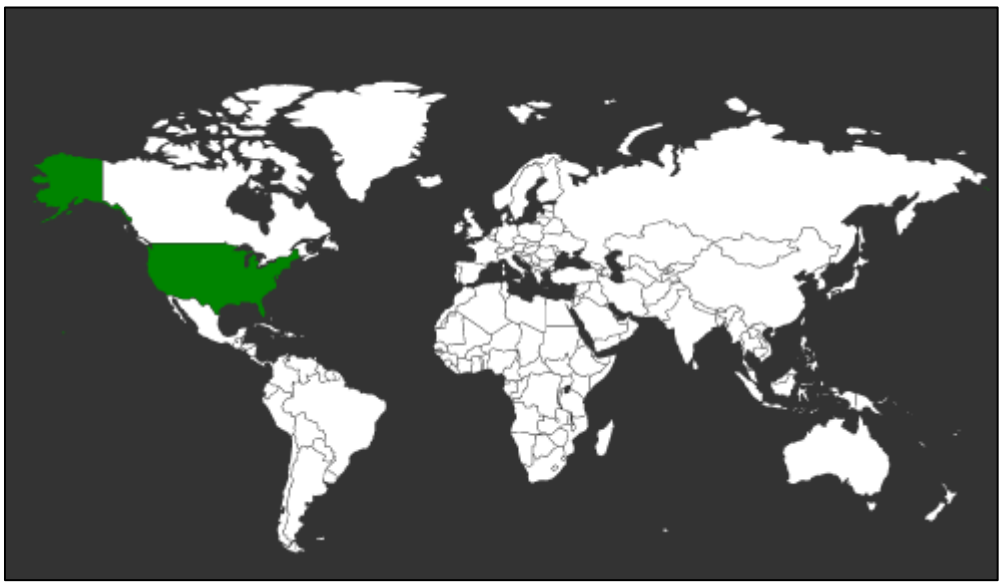
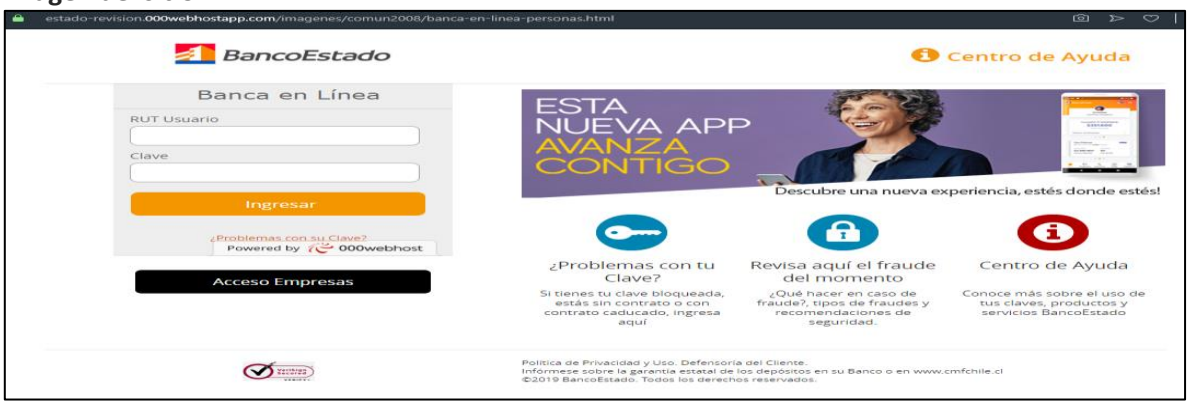
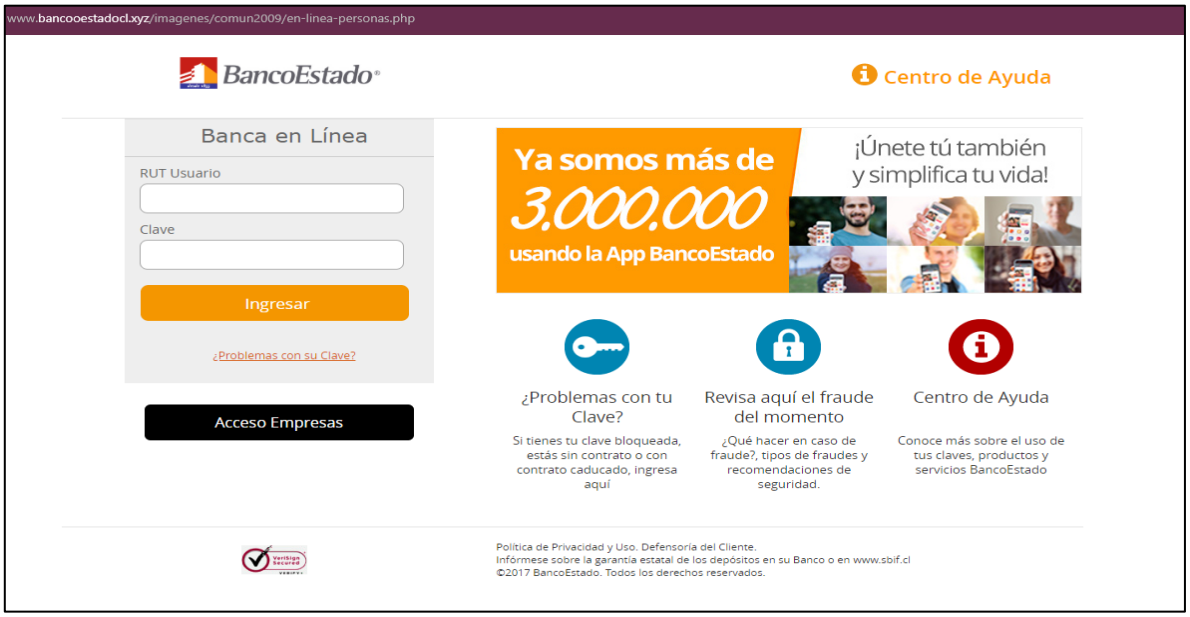
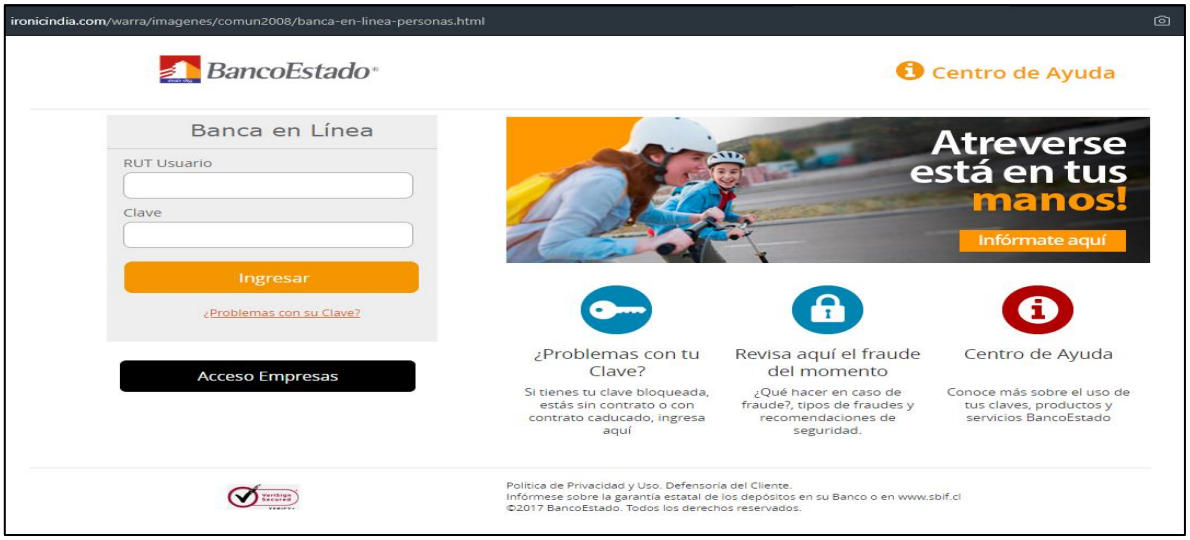


**Imagen del sitio**






## Whois

```
soc@ITQ-ivps3:~$ whois 000webhostapp.com
   Domain Name: 000WEBHOSTAPP.COM
   Registry Domain ID: 2027404438_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.hostinger.com
   Registrar URL: http://www.hostinger.com
   Updated Date: 2017-04-05T08:04:14Z
   Creation Date: 2016-05-11T13:34:12Z
   Registry Expiry Date: 2022-05-11T13:34:12Z
   Registrar: Hostinger, UAB
   Registrar IANA ID: 1636
   Registrar Abuse Contact Email: abuse@hostinger.com
   Registrar Abuse Contact Phone: +37064503378
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: DNS1.000WEBHOST.COM
   Name Server: DNS2.000WEBHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-10-16T15:11:12Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

```
Domain Name: bancooestadocl.xyz
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2019-10-15T07:00:00Z
Creation Date: 2019-10-15T07:00:00Z
Registrar Registration Expiration Date: 2020-10-15T07:00:00Z
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-ee4c63a9eb773575696964e748736bc8@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-ee4c63a9eb773575696964e748736bc8@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-ee4c63a9eb773575696964e748736bc8@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: 2019-10-15T07:00:00Z <<<
```

```
soc@ITQ-ivps3:~$ whois ironicindia.com
   Domain Name: IRONICINDIA.COM
   Registry Domain ID: 2437051410_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2019-09-25T16:43:25Z
   Creation Date: 2019-09-25T16:30:19Z
   Registry Expiry Date: 2020-09-25T16:30:19Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: CNS33.WEBHOSTBOX.NET
   Name Server: CNS34.WEBHOSTBOX.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-10-16T17:13:27Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

**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: 2019.10.17 09:43:00 -03'00'